THE PORT AUTHORITY OF NY & NJ

PROCUREMENT DEPARTMENT
ATTN: BID/PROPOSAL CUSTODIAN
4 WORLD TRADE CENTER
150 GREENWICH STREET, 21ST Floor
NEW YORK, NY 10007

REQUEST FOR PROPOSALS

ISSUE DATE: **March 22, 2016**

TITLE: **PARKING ACCESS AND REVENUE CONTROL SYSTEM – DESIGN, INSTALLATION AND MAINTENANCE AT JOHN F. KENNEDY INTERNATIONAL AIRPORT, NEWARK LIBERTY INTERNATIONAL AIRPORT, LAGUARDIA AIRPORT AND STEWART INTERNATIONAL AIRPORT**

RFP NO.: **45551**

SUBMIT PROPOSALS NO LATER THAN THE DUE DATE AND TIME TO THE ABOVE ADDRESS

PRE-PROPOSAL MEETING: **April 11, 2016** **TIME: 9:00 A.M**
Location: John F. Kennedy International Airport, Building 14, Lobby, Queens, NY 11430

FACILITY INSPECTION:

i. John F. Kennedy International Airport, Building 14, Lobby 10:00 am, Monday, April 11, 2016
ii. Newark Liberty International Airport, Building 1, Lobby 9:00 am Tuesday, April 12, 2016
iii. Stewart International Airport, 1180 First Street, Building 138, New Windsor, NY 12553 10:00 am Wednesday, April 13, 2016
iv. LaGuardia Airport, Hangar 7, 3rd Floor 9:00 am Thursday, April 14, 2016

QUESTIONS DUE BY: **April 21, 2016** **TIME: 3:00 P.M**

PROPOSAL DUE DATE: **May 26, 2016** **TIME: 2:00 P.M.**

CONTACT: **Jeanette Anderson** **PHONE:** (212) 435-4624
EMAIL: **jeanette.anderson@panynj.gov** **FAX:** (212) 435-4695

Parking Access and Revenue Control System—Design, Installation & Maintenance

1) INFORMATION FOR PROPOSERS ON THIS REQUEST FOR PROPOSALS

a) General Information: The Port Authority of New York and New Jersey

The Port Authority of New York and New Jersey (the "Port Authority" or the "Authority") is an agency of the States of New York and New Jersey, created and existing by virtue of the Compact of April 30, 1921, made by and between the two States, and thereafter consented to by the Congress of the United States. It is charged with providing transportation, terminal and other facilities of trade and commerce within the Port District. The Port District comprises and area of about 1,500 square miles in both States, centering about New York Harbor. The Port District includes the Cities of New York and Yonkers in New York State, and the cities of Newark, Jersey City, Bayonne, Hoboken and Elizabeth in the State of New Jersey, and over 200 other municipalities, including all or part of seventeen counties, in the two States. The Port Authority manages and/or operates all of the region's major commercial airports (Newark Liberty International, John F. Kennedy International, Teterboro, LaGuardia and Stewart International Airports), marine terminals in both New Jersey and New York (Port Newark and Elizabeth, Howland Hook and Brooklyn Piers); and its interstate tunnels and bridges (the Lincoln and Holland Tunnels; the George Washington, Bayonne, and Goethals Bridges; and the Outerbridge Crossing), which are vital "Gateways to the Nation."

In addition, the Port Authority operates the Port Authority Bus Terminal in Manhattan, the largest facility of its kind in the world, and the George Washington Bridge and Journal Square Transportation Center bus stations. A key link in interstate commuter travel, the Port Authority also operates the Port Authority Trans-Hudson Corporation (PATH), a rapid rail transit system linking Newark, and the Jersey City and Hoboken waterfronts, with midtown and downtown Manhattan. A number of other key properties are managed by the agency including but not limited to a large satellite communications facility (the Teleport) in Staten Island, and a resource recovery co-generation plant in Newark. Prior to September 11, 2001, the Port Authority's headquarters were located in the World Trade Center, and that complex is still owned and being partially redeveloped by the Authority.

The Port Authority is hereby seeking proposals from qualified firms to provide a fully functional airport Parking Access and Revenue Control System (PARCS) for John F. Kennedy International Airport (JFK), LaGuardia Airport (LGA), Newark Liberty International Airport (EWR), and Stewart International Airport (SWF), including Parking Access and Revenue Control System Design, Implementation and Maintenance, as more fully described herein.

b) Brief Summary of Scope of Work

The Contractor shall provide a fully functional airport Parking Access and Revenue Control System (PARCS) for John F. Kennedy International Airport (JFK), LaGuardia Airport (LGA), Newark Liberty International Airport (EWR), and Stewart International Airport (SWF).

The Contractor's responsibilities shall include, but not be limited to, the following:

i) design and implement a PARCS that meets the functional specifications enumerated in Attachment E, "Functional Specifications", to serve parking operations at John F. Kennedy International Airport, LaGuardia Airport, Newark Liberty International Airport, and Stewart Airport.
ii) provide preventative and remedial system maintenance (with availability of twenty-four hours a day, seven days a week) of all equipment, hardware, and software necessary to maintain the operation and use of the PARCS.
iii) provide services and materials for the maintenance, operation, and replacement of all existing PARCS hardware, software and the local area network communications equipment (at each entry and exit plaza) that constitute the four separate systems currently serving airport parking operations at John F. Kennedy International Airport, LaGuardia Airport, Newark Liberty International Airport, and Stewart International Airport.
iv) maintain and ensure operational functionality of the Existing PARCS at each airport until the transition to the New PARCS at each airport is fully installed, accepted and fully operational.
v) decommission and remove the Existing PARCS at each airport upon a fully installed, accepted and fully operational New PARCS.
vi) provide training as required to implement the system.

Please refer to Attachment D: "Scope of Work" for full description of services required under this Contract.

c) Deadline for Receipt of Proposals

The due date specified on the cover page is the May 26, 2016. Closing of due date is 2:00 P.M., Eastern Standard Time (EST).

PLEASE READ THE FOLLOWING DELIVERY REQUIREMENTS CAREFULLY. Proposers assume all responsibility for delays or problems in delivery.

Proposal submissions will be received at:

The Port Authority of NY & NJ
Attention: Proposal Custodian
Procurement Department
4 World Trade Center
150 Greenwich Street, 21st Floor
New York, NY 10007

Clearly mark the solicitation number on the outermost package.

At this address, proposals will be accepted via (1) regular mail, (2) express delivery service (e.g. UPS), or (3) hand delivery.

Express carrier deliveries by commercial vehicles can be made via vendors approved by Silverstein Properties, the 4 World Trade Center (4 WTC) Property Manager, through the Vehicle Security Center (VSC). Presently, UPS is the only delivery vendor with approved recurring delivery times.

There is extensive security at the World Trade Center Site. Individuals must present a valid government-issued photo ID to enter 4 WTC. Individuals without valid identification shall be turned away and their packages not accepted. Individuals without packages or carrying small packages or boxes that can be conveyed by hand or on a hand truck may enter through the lobby. All envelopes, packages and boxes may be subject to additional security screening.

There is no parking available at 4 WTC/150 Greenwich Street, and parking in the surrounding area is extremely limited.

The Port Authority assumes no responsibility for delays caused by any delivery service.

d) Vendor Profile

To ensure maximum opportunities, it is vitally important that Proposers keep their vendor profiles up to date with an appropriate e-mail address, as this will enable their firm to receive timely notice of advertisements, reminders, solicitations and addenda. Proposers may update their vendor profile or register as a Port Authority Vendor by accessing the online registration system at https://panynjprocure.com/VenLogon.asp.

e) Submission of Proposals

One reproducible original (containing original signatures and clearly designated as such) and thirty (30) double-sided copies of the proposal must be submitted on or before the due date and time in accordance with the information on the cover page of this RFP and sent or delivered to the RFP Custodian at the address specified on the cover page. Each copy of the proposal as well as the parcel(s) used for shipping must be conspicuously marked with the Proposer's name and address as well as the Proposer's Vendor Number, if available. In addition, the outside of the package must clearly state the title of this RFP, the number of this RFP and the Proposal Due Date. Failure to properly label proposal submissions may cause a delay in identification, misdirection or disqualification of proposal submissions.

Consistent with environmentally preferable procurement practices, the Port Authority requests all documents submitted to be in a form that can be easily recycled (i.e., no plastic

covers or binding) and to provide only supporting literature which directly relates to the proposal being submitted.

f) Communications Regarding this RFP

All communications concerning this RFP should be directed to the Contracts Specialist listed on the cover page. All questions regarding this RFP should be submitted in writing to the Contracts Specialist at the address or facsimile number listed on the cover page no later than **3:00 p.m. (EST) on (April 21st, 2016).**

The Contracts Specialist is authorized only to direct the attention of prospective Proposers to various portions of this RFP so that they may read and interpret such portions themselves.

Neither the Contracts Specialist nor any other employee of the Port Authority is authorized to interpret the provisions of this RFP or give additional information as to its requirements. If interpretation or other information is required, it will be communicated to Proposers by written addenda and such writing shall form a part of this RFP.

g) Proposal Acceptance or Rejection

Acceptance shall be only by mailing to or delivering at the office designated by the Proposer in its proposal, a notice in writing signed by an authorized representative on behalf of the Port Authority specifically stating that the proposal is accepted or by execution of an agreement covering the subject matter of this RFP signed by authorized representatives of the Port Authority and the Proposer. No other act of the Port Authority, its Commissioners, officers, agents, representatives, or employees shall constitute acceptance of a proposal. Rejection of a proposal shall be only by either (a) a notice in writing specifically stating that the proposal is not accepted, signed by an authorized representative of the Port Authority and mailed to or delivered to the Proposer at the office designated in the Proposal, or (b) omission of the Port Authority to accept the proposal within 180 days after the Proposal Due Date. No other act of the Port Authority, its Commissioners, officers, agents, representatives or employees shall constitute rejection of a proposal.

h) Union Jurisdiction

Proposers are advised to ascertain whether any union now represented or not represented at the facility will claim jurisdiction over any aspect of the operations to be performed hereunder and their attention is directed to the Section of this RFP entitled “Harmony” included in the “General Contract Provisions” hereunder.

i) City Payroll Tax

Proposers should be aware of the payroll tax imposed by the:

i) City of Newark, New Jersey for services performed in Newark, New Jersey
ii) City of Elizabeth, New Jersey for services performed in Elizabeth, New Jersey
iii) City of New York, New York for services performed in New York, New York
iv) City of Newburgh, New York for services performed in Newburgh, New York

These taxes, if applicable, are the sole responsibility of the Contractor. Proposers should consult their tax advisors as to the effect, if any, of these taxes. The Port Authority provides this notice for informational purposes only and is not responsible for either the imposition or administration of such taxes. The Port Authority exemption set forth in the Paragraph headed "Sales or Compensating Use Taxes", in the Standard Contract Terms and Conditions included herein, does not apply to these taxes.

j) Pre-Proposal Meeting

A Pre-Proposal Meeting is scheduled for 9am, Monday, April 11, 2016 at John F. Kennedy International Airport, Building 14, Lobby.

Any questions concerning this RFP should be submitted in writing prior to the meeting so that the Port Authority may prepare responses in advance of the meeting. Additional questions may be permitted at the meeting; however, responses may be deferred and provided at a later date by written addenda.

k) Site Inspection

Facility Inspections are scheduled as follows:

i. John F. Kennedy International Airport, Building 14, Lobby 10am, Monday, April 11, 2016
ii. Newark Liberty International Airport, Building 1, Lobby 9am Tuesday, April 12, 2016
iii. Stewart International Airport, 1180 First Street, Building 138, New Windsor, NY 12553 10am Wednesday, April 13, 2016
iv. LaGuardia Airport, Hangar 7, 3rd Floor 9am Thursday, April 14, 2016

A site inspection allows Proposers to tour and physically inspect the actual site(s) of work prior to the submission of proposals. Proposers may wish to measure such things as cashier booths and existing equipment cabinets. In addition, system components such as PCs will be available for inspection. Proposers will be shown the central and backup data centers, parking operations offices and the entrance and exit plazas as well as other field equipment. No questions will be taken during a site inspection.

Attendance is strongly recommended. Information conveyed may be useful to Proposers in preparing their proposals and Proposers not attending assume all risks which may ensue from non-attendance. Maximum two (2) individuals per Proposer are allowed to attend. Two (2) valid forms of photo ID are required with one form being a driver license/state

identification card or passport to attend the site inspection. Attendees interested in attending should RSVP to Kyle Sundin, Manager, Airport Parking and Revenue Systems, via email at ksundin@panynj.gov no later than 12 noon (EST) of the business day preceding the schedule date(s) to confirm their attendance and/or receive travel directions.

l) Available Documents

The below listed documents will be available for Proposers to examine. These documents were not prepared for the purpose of providing information for Proposers on this RFP but they were prepared for other purposes, such as for other contracts or for design purposes for this or other contracts, and they do not form a part of this RFP. The Port Authority makes no representation or guarantee as to, and shall not be responsible for, their accuracy, completeness or pertinence, and, in addition, shall not be responsible for inferences or conclusions drawn there from. They are made available to Proposers merely for the purpose of providing them with such information, whether or not such information may be accurate, complete, pertinent or of any value to Proposers.

Said documents are as follows:

i) LaGuardia Airport as-built drawings and/or design drawings depending upon availability.
ii) John F. Kennedy International Airport as-built drawings and/or design drawings depending upon availability.
iii) Newark Liberty International Airport as-built drawings and/or design drawings depending upon availability.
iv) Existing Contracts for Current System Maintenance and Enhancement Procurement.
v) System Administration Manual for Port Authority Technology (Protected Information as defined in the Information Security Handbook).

Completion and submittal of the attached Non Disclosure Agreement is required prior to document review (see Attachment V).

Document viewing will be held from 10am to 4pm on April 15, 21 and 22, 2016 at 4 World Trade Center, 150 Greenwich St, Aviation Department, 18th Floor, New York, NY 10007. Contact Kyle Sundin ksundin@panynj.gov or 212.435.3804 to schedule a time for viewing.

A reading room will be provided to review the technical documents and drawings. No cameras and photocopying of materials are allowed during the inspection. Individuals are limited to a 90 minute document review period.

Proposers must complete and sign a Non-Disclosure and Confidentiality Agreement (Attachment V). The NDA must be signed by an individual authorized to bind the company and presented in unaltered form by noon, April 7, 2016 prior to viewing any

documents. The original NDAs MUST be received by the Port Authority prior to allowing access to the Documents.

Fully executed original NDAs MUST be provided to Jeanette Anderson (Jeanette.anderson@panynj.gov) prior to being permitted to view the documents at the document inspection visit. The Port Authority of New York and New Jersey "Information Security Handbook" referenced in the aforementioned NDA can be found as Attachment O.

m) Additional Proposer Information

Prospective Proposers are advised that additional vendor information, including, but not limited to forms, documents and other information, including M/WBE Participation Plan Submission Forms and protest procedures, may be found on the Port Authority website at: http://www.panynj.gov/business-opportunities/become-vendor.html

n) Contractor Staff Background Screening

The Contractor awarded this contract will be required to have its staff, and any subcontractor's staff working under this Contract, authorize the Authority or its designee to perform background checks. Such authorization shall be in a form acceptable to the Authority. The Contractor (and subcontractor) may also be required to use an organization designated by the Authority to perform the background checks. The cost for said background checks for staff that pass and are granted a credential shall be reimbursable to the Contractor (and its subcontractors) as an out-of-pocket expense as provided herein. Staff that are rejected for a credential for any reason are not reimbursable.

As of January 29, 2007, the Secure Worker Access Consortium (S.W.A.C.) is the only Port Authority approved provider to be used to conduct background screening, except as otherwise required by federal law and/or regulation. Information about S.W.A.C., instructions, corporate enrollment, online applications, and location of processing centers can be found at http://www.secureworker.com, or S.W.A.C. may be contacted directly at (877)522-7922.

o) Automated Clearing House Enrollment

The Port Authority of New York and New Jersey is transitioning to an all electronic method of paying its vendors and contractors via an Automated Clearing House (ACH) funds transfer. The Contractor must complete the Port Authority's "Authorization Agreement For Direct Deposits And Direct Payments (ACH Credits)" form, which is available at http://www.panynj.gov/business-opportunities/pdf/ach-authorization-form.pdf, in order to receive payment. To avoid delays in payments for commodities and services provided, vendors and contractors must be enrolled in ACH. Printed accounts payable checks will not be issued. The Authorization Agreement shall remain in full force and effect until the Port

Authority has received written notification from the Contractor of its termination in such time and in such manner as to afford the Port Authority and the depository financial institution(s) a reasonable opportunity to act on it. Any questions on this initiative may be directed to the ACH Enrollments contact line at 201 216-6002 or emailed to ACHENROLLMENT@PANYNJ.GOV.

2) DOCUMENTATION CONSTRUCTION AND INTERPRETATION

In the event of any conflict, ambiguity or inconsistency between or among any of the provisions in this Agreement the Manager shall determine which provision will apply.

3) SCOPE OF WORK

The full Scope of Work is set forth in detail in Attachment D.

4) PROPOSER PREREQUISITES

Only Proposers who can demonstrate that they comply with the following should submit proposals as only proposals from such Proposers will be considered. Proof of meeting the following prerequisites must be submitted using the form provided as Attachment X hereof: supporting documentation must be submitted in a clear and concise manner as part of the Proposer Prerequisites response.

a) The Proposer shall have had at least three (3) years of continuous experience immediately prior to the date of the submission of its proposal in the management and operation of at least one Parking Access and Revenue Control System (PARCS), which includes design, implementation and maintenance. The Proposer may fulfill this prerequisite if it can demonstrate that the persons or entities owning and controlling the Proposer have had a cumulative total of at least the same number of years and type of direct continuous experience immediately prior to the submission of this proposal as is required of the Proposer, or has owned and controlled other entities which meet the requirement.

b) During the time period stated in (a) above, the Proposer shall demonstrate satisfactory performance of at least two (2) contracts for similar services of similar scope supporting airport parking facilities that process at least 2,500,000 parking and revenue transactions annually and/or have at least 7,000 parking spaces.

If the Proposer intends to utilize a subcontractor, the Proposer may apply the relevant experience of that subcontractor towards the experience required for the prerequisite above.

In the event a proposal is submitted by a joint venture, the foregoing prerequisites will be considered with respect to such Proposal as follows:

With respect to subparagraphs (a) and (b) above, the prerequisites will be considered satisfied if the joint venture itself, or any of its participants individually, can meet the requirements.

If the proposal is submitted by a common law joint venture, a joint venture that has not been established as a distinct legal entity, each participant of the joint venture shall be held jointly and severally liable and must individually execute and perform all acts required by this proposal. Documents signed by a common law joint venture, in connection with this proposal, shall include the names of all participants of the joint venture followed by the words "acting jointly and severally". All joint venture proposers must provide documentation of their legal status.

All Proposers must include documentation that they meet the above prerequisites.

By furnishing this solicitation document to Proposers, the Port Authority has not made a determination that the Proposers have met the prerequisites or have otherwise been deemed qualified to perform the services. In addition, a determination that a Proposer has met the prerequisites is no assurance that they will be deemed qualified in connection with other proposal requirements included herein.

5) FINANCIAL INFORMATION

The Proposer will be required to demonstrate that it is financially capable of performing the contract resulting from this RFP ("Contract"). The determination of the Proposer's financial qualifications and ability to perform this Contract will be in the sole discretion of the Port Authority. The Proposer shall submit, with its proposal, the following:

a) Certified financial statements

i) Certified financial statements, including applicable notes, reflecting the Proposer's assets, liabilities, net worth, revenues, expenses, profit or loss and cash flow for the most recent year or the Proposer's most recent fiscal year.

ii) Where the certified financial statements in (i) are not available, then reviewed statements from an independent accountant setting forth the aforementioned information shall be provided.

Where the statements submitted pursuant to subparagraphs (i) and (ii) aforementioned do not cover a period which includes a date not more than forty-five days prior to the Proposal Due Date, then the Proposer shall also submit a statement in writing, signed by an executive officer or his/her designee, that the present financial condition of the Proposer is at least as good as that shown on the statements submitted.

b) A statement of work which the Proposer has on hand, including any work on which a bid and/or proposal has been submitted, containing a description of the work, the annual dollar value, the location by City and State, the current percentage of completion, the expected date for completion, and the name of an individual most familiar with the Proposer's work on these jobs.

c) The name and address of the Proposer's banking institution, chief banking representative handling the Proposer's account, the Proposer's Federal Employer Identification Number (i.e., the number assigned to firms by the Federal Government for tax purposes), the Proposer's Dun and Bradstreet number, if any, the name of any credit service to which the Proposer furnished information and the number, if any, assigned by such service to the Proposer's account.

6) EVALUATION CRITERIA AND RANKING

The Proposer must submit a proposal that details and clearly describes its experience and capability to perform the services described in this RFP, its approach to such work and the cost of such work to the Authority. Note: Criteria B and C are weighted equally. At a minimum, the proposal must address and be organized according to the following criteria:

a) Technical Plan & Work Approach:

- The degree to which the features and functions of the proposed PARCS meet the stated functional requirements and objectives as described in Attachment D, "Scope of Work" and Attachment E, "Functional Requirement" in the RFP will be evaluated as follows:
  - Staffing Plans—The extent to which the Proposer, and the managerial and supervisory personnel proposed to be dedicated to this Contract have the demonstrated technical expertise and understanding of implementing, maintaining and operating similar services in similar environments.
  - Quality of start-up approach and business transition plan for start of Contract and termination of Contract.
  - Approach to new hardware installation and implementation of software solutions to meet goals and objectives of the Port Authority as described in Attachment D, "Scope of Work" and Attachment E, "Functional Requirements" of this RFP.
  - Standard operating procedures related to System development, installation and maintenance support.
  - Approach to Maintenance Management Reporting.
  - Approach of each heading in the Scope of Work (Attachment D) and Functional Requirements (Attachment D) of this RFP.

- The degree to which the Proposer's Implementation Schedule enables an expedient transition from the Existing PARCS to the New PARCS.

b) Cost Proposal
The degree to which the services and product required by this RFP are cost effective to the Authority and the overall cost of the proposed System and Services. The Proposer shall submit a Cost Proposal indicating the compensation that it expects to receive. The Cost Proposal shall be complete and inclusive of all work required by this RFP, including but not be limited to: installation costs, equipment removal and transition costs, monthly maintenance costs, material and labor costs, fuel costs, any salaries, health benefits and other benefits, overheads, profits, etc. Proposer shall submit the Cost Proposal utilizing Attachment C2 attached herein.

c) Management / Firm Experience and Qualifications Approach
The experience, qualifications and availability of the management and staff proposed to be assigned to provide the services (including subcontractors, if any) will be evaluated in the Management/Qualification Approach section including the following:

- A description of how the Proposer intends to staff, implement and manage the required services hereunder, including any information that it believes would be helpful to the Port Authority in assessing its management approach and ability to provide the services.
- The Proposer's management philosophy and approach to performing the subject services, which shall include, but is not limited to, the following:
  a) An organization chart for this project that identifies the relationship between the Project Manager, Principals and other key individuals. Include their titles, office address, function, task responsibility and overall reporting relationships.
  b) A profile of each person identified in the organization chart that describes how his or her experience and technical capabilities will assist in the successful performance and completion of the Contract. Include the number and relevant experience of all managerial and supervisory personnel proposed to be dedicated to the Contract.
  c) Approach to keeping the Authority informed of any issues and progress during performance of the contemplated services.
- Nature and quality of the Proposer's Quality Assurance/Quality Control Program.
- The Proposer's maintenance and training methodology.
- The quality and extent of financial, reconciliation and auditing procedures.
- Prior experience between firms proposing a joint venture and prime subcontractor relationship.
- The Proposer's Disaster Recovery Plan.
- The quality and effectiveness of the Proposer's MBE/WBE Plan, Certification of Environmentally Preferable Products/Practices, and subcontracting plan and the extent to which it meets or exceeds Port Authority Standards.

- The capability of managerial, technical and physical resources to deliver the required services over an extended period of time.
- The Proposer's commitment to provide the requested services, to meet or exceed all requirements which include: the capability of the Proposer to meet all requirements of the RFP, including but not limited to the firm's ability to comply with the insurance requirements and General Contract Provisions and Contract Specific Terms and Conditions.

d) Background Check Plan
The Proposer must submit a Background Check plan in accordance with this document, which will be considered "pass/fail."

e) Business Risk
Consideration will be given to the degree of business risk assumed by the Port Authority. This will include, but not be limited to, assessment of the impact resulting from the possible failure of the Contractor to perform under the terms and conditions of this Contract. As part of the evaluation, business risk will also be measured by the Port Authority's assessment of its ability to immediately replace the Contractor in a manner that maintains or improves the quality and continuity of facility for the PARCS System required herein.

7) MBE/WBE SUBCONTRACTING PROVISIONS

The Port Authority has a long-standing practice of making its business opportunities available to Minority Business Enterprises (MBEs) and Woman-owned Businesses (WBEs) and has taken affirmative steps to encourage such firms to seek business opportunities with the Port Authority. The successful Proposer will use good faith efforts to provide for meaningful participation by the Port Authority Port Authority certified MBE/WBEs as defined in this document, in the purchasing and subcontracting opportunities associated with this contract, including purchase of equipment, supplies and labor services.

MBE/WBE Good Faith Participation – The Contractor shall use every good-faith effort to provide for participation by Port Authority certified Minority Business Enterprises (MBEs) and Port Authority certified Woman-owned Business Enterprises (WBEs) in all purchasing and subcontracting opportunities associated with this Contract, including purchase of equipment, supplies and labor services, in accordance with the section of the Standard Terms and Conditions entitled "MBE/WBE Good Faith Participation."

The Contractor shall use good faith efforts to achieve participation equivalent to twelve percent (12%) of the total Contract price for MBEs and five percent (5%) of the total Contract price for WBEs.

Good faith efforts to include participation by MBE/WBEs shall include, but not be limited to the following:

i) Dividing the services and materials to be procured into small portions, where feasible.
ii) Giving reasonable advance notice of specific contracting, subcontracting and purchasing opportunities to such MBE/WBEs as may be appropriate.
iii) Soliciting services and materials from a Port Authority Port Authority certified MBE/WBE or seeking MBE/WBEs from other sources. To access the Port Authority's Directory of MBE/WBE Port Authority certified Firms go to www.panynj.gov/supplierdiversty
iv) Ensuring that provision is made to provide progress payments to MBE/WBEs on a timely basis.
v) Observance of reasonable commercial standards of fair dealing in the respective trade or business.

Proposers are directed to use form PA3760C as the recording mechanism for the MBE/WBE participation plan, annexed hereto as Attachment G, MBE/WBE Subcontracting Plan or may be downloaded at http://www.panynj.gov/business-opportunities/become-vendor.html.

Proposers shall include their MBE/WBE Participation Plan with their Proposals, to be reviewed and approved by the Authority's Office of Business Diversity and Civil Rights (OBDCR).

The MBE/WBE Plan submitted by the Contractor to the Port Authority shall contain, at a minimum, the following:

i) Identification of MBE/WBEs: Provide the names and addresses of all MBE/WBEs included in the Plan. If none are identified, describe the process for selecting participant firms in order to achieve the good faith goals under this Contract.
ii) Level of Participation: Indicate the percentage of MBE/WBE participation expected to be achieved with the arrangement described in the Plan.
iii) Scope of Work: Describe the specific scope of work the MBE/WBEs will perform.

All MBE/WBE subcontractors listed on the MBE/WBE Participation Plan must be certified by the Port Authority in order for the Contractor to receive credit toward the MBE/WBE goals set forth in this Contract. Please go to http://www.panynj.gov/business-opportunities/supplier-diversity.html to search for MBE/WBEs by a particular commodity or service. The Port Authority makes no representation as to the financial responsibility of these firms or their ability to perform work under this Contract.

Subsequent to Contract award, all changes to the MBE/WBE Participation Plan must be submitted via a modified MBE/WBE Participation Plan to the Manager for review and approval by the Authority's Office of Business Diversity and Civil Rights. For submittal of modifications to the MBE/WBE Plan, Contractors are directed to use form PA3760D, which may be downloaded at http://www.panynj.gov/business-opportunities/become-vendor.html. The Contractor shall not make changes to its approved MBE/WBE Participation Plan or substitute MBE/WBE subcontractors or suppliers for those named in their approved plan without the Manager's prior written approval. Unauthorized changes

or substitutions, including performing the work designated for a subcontractor with the Contractor's own forces, shall be a violation of this section. Progress toward attainment of MBE/WBE participation goals set forth herein will be monitored throughout the duration of this Contract.

The Contractor shall also submit to the Manager, along with invoices, the Statement of Subcontractor Payments in the form of the MBE/WBE Participation Report, which may be downloaded at http://www.panynj.gov/business-opportunities/become-vendor.html. The Statement must include the name and business address of each MBE/WBE subcontractor and supplier actually involved in the Contract, a description of the work performed and/or product or service supplied by each such subcontractor or supplier, the date and amount of each expenditure, and such other information that may assist the Manager in determining the Contractor's compliance with the foregoing provisions.

a) Prompt Payment/Retainage

The Contractor agrees to pay each subcontractor under this Contract, for satisfactory performance of its subcontract, no later than ten (10) days from the receipt of each payment the Contractor receives from the Authority. The prime contractor agrees further to return retainage payments, if any to each subcontractor within ten (10) days after the subcontractors' work is satisfactorily completed. Any delay or postponement of payment from the above referenced timeframe may occur only for good cause following written approval of the Authority.

b) MBE/WBE Conditions of Participation

MBE/WBE participation will be counted toward meeting the MBE/WBE contract goal, subject to all of the following conditions:

i) Commercially Useful Function. An MBE/WBE is considered to perform a commercially useful function when it is responsible for the execution of a distinct element of work on a contract and carries out its responsibilities by actually performing, managing, and supervising the work involved in accordance with normal industry practice. Regardless of whether an arrangement between the Contractor and the MBE/WBE represent standard industry practice, if the arrangement erodes the ownership, control or independence of the MBE/WBE or in any other way does not meet the commercially useful function requirement, that firm shall not be included in determining whether the MBE/WBE goal is met and shall not be included in MBE/WBE reports. If this occurs with respect to a firm identified as a MBE/WBE, the Contractor shall receive no credit toward the MBE/WBE goal and may be required to backfill the participation. An MBE/WBE does not perform a commercially useful function if its role is limited to that of an extra participant in a transaction or contract through which funds are passed in order to obtain the appearance of MBE/WBE participation. An MBE/WBE may rebut a determination by the Authority

that the MBE/WBE is not performing a commercially useful function to the Authority.

ii) Work Force. The MBE/WBE must employ a work force (including administrative and clerical staff) separate and apart from that employed by the Contractor, other Subcontractors on the contract, or their Affiliates. This does not preclude the employment by the MBE/WBE of an individual that has been previously employed by another firm involved in the Contract, provided that the individual was independently recruited by the MBE/WBE in accordance with customary industry practice. The routine transfer of work crews from another employer to the MBE/WBE shall not be allowed.

iii) Supervision. All Work performed by the MBE/WBE must be controlled and supervised by the MBE/WBE without duplication of supervisory personnel from the Contractor, other Subcontractors on the contract, or their Affiliates. This does not preclude routine communication between the supervisory personnel of the MBE/WBE and other supervisors necessary to coordinate the Work.

c) Counting MBE/WBE Participation

The value of the Work performed by an MBE/WBE, with its own equipment, with its own forces, and under its own supervision will be counted toward the goal, provided the utilization is a commercially useful function. An MBE/WBE prime contractor shall still provide opportunities for participation by other MBE/WBEs. Work performed by MBE/WBEs will be counted as set forth below. If the Authority determines that some or all of the MBE/WBEs work does not constitute a commercially useful function, only the portion of the work considered to be a commercially useful function will be credited toward the goal.

i) Subcontractors. One hundred percent (100%) of the value of the Work to be performed by an MBE/WBE subcontractor will be counted toward the MBE/WBE goal. The value of such Work includes the cost of materials and supplies purchased by the MBE/WBE, except the cost of supplies or equipment leased from the Contractor, other Subcontractors or their affiliates will not be counted. When a MBE/WBE subcontracts part of the work of its contract to another firm, the value of the subcontracted work may be counted toward MBE/WBE goals only if the MBE/WBE subcontractor is itself a MBE/WBE. Work that a MBE/WBE subcontracts to a non-MBE/WBE firm does not count toward MBE/WBE goals.

ii) Manufacturers/Fabricators. One hundred percent (100%) of the expenditure to a MBE/WBE manufacturer or fabricator will be counted towards the MBE/WBE goal.

iii) Material Suppliers. Sixty percent (60%) of the expenditure to a MBE/WBE material supplier will be counted toward the MBE/WBE goal. Packagers, brokers,

manufacturer's representatives, or other persons who arrange or expedite transactions are not material suppliers within the meaning of this paragraph.

iv) Broker's/Manufacturer's Representatives. One hundred percent (100%) of fees or commissions charged for assistance in the procurement of the materials and supplies, or fees for transportation charges for the delivery of materials or supplies provided by an MBE/WBE broker/manufacturer's representative will be counted toward the MBE/WBE goal, provided they are determined by the Authority to be reasonable and not excessive as compared with fees customarily allowed for similar services. The cost of the materials and supplies themselves will not be counted.

v) Services. One hundred percent (100%) of fees or commissions charged by an MBE/WBE for providing a bona fide service, such as professional, technical, consultant, or managerial services, or for providing bonds or insurance specifically required for the performance of the Work will be counted toward the MBE/WBE goal, provided the fee is reasonable and not excessive as compared with fees customarily allowed for similar services.

vi) Trucking Operations. If using an MBE/WBE firm for trucking operations, the MBE/WBE trucking firm of record is the firm that is listed on the MBE/WBE Participation Plan. The MBE/WBE trucking firm shall own and operate at least one registered, insured, and fully operational truck used for the performance of the Work and shall be responsible for the management and supervision of the entire trucking operation for which it is responsible on a particular contract, and there cannot be a contrived arrangement for the purpose of meeting the MBE/WBE goal. The MBE/WBE trucking firm of record shall control the day-to-day MBE/WBE trucking operations for performance of the Work, and shall be responsible for (1) negotiating and executing rental/leasing agreements; (2) hiring and terminating the work force; (3) coordinating the daily trucking needs with the Contractor; and (4) scheduling and dispatching trucks.

vii) MBE/WBE Short-Term Leased Trucks. The MBE/WBE may lease trucks on a short-term basis from another MBE/WBE, including an owner/operator who is Port Authority certified as a MBE/WBE. 100% of the value of the trucking operations that the lessee MBE/WBE provides will be counted toward the MBE/WBE goal.

viii) Non-MBE/WBE Trucks. The MBE/WBE may lease trucks on a short-term basis from a non-MBE/WBE, including an owner-operator. One hundred percent (100%) of the fee or commission the MBE/WBE receives as a result of the lease arrangement will be counted toward the MBE/WBE goal. The value of the trucking operations provided by the lessee will not be counted toward the MBE/WBE goal.

ix) Joint ventures between MBE/WBEs and non-MBE/WBEs may be counted toward the MBE/WBE goal in proportion to the total dollar value of the contract equal to the

distinct, clearly defined portion of the work of the contract that the MBE/WBE performs with its own forces. Please contact the Office of Business Diversity and Civil Rights at (201) 395-3958 for more information about requirements for such joint ventures.

5) CERTIFICATION OF RECYCLED MATERIALS PROVISION

Proposers shall submit, with their proposal, Attachment H, the Certified Environmentally Preferable Products / Practices Form attesting that the products or items offered by the Proposer contain the minimum percentage of post-consumer recovered material in accordance with the most recent guidelines issued by the United States Environmental Protection Agency (EPA), or, for commodities not so covered, the minimum percentage of post-consumer recovered materials established by other applicable regulatory agencies.

Recycling Definitions:

For purposes of this solicitation, the following definitions shall apply:

a) "Recovered Material" shall be defined as any waste material or by-product that has been recovered or diverted from solid waste, excluding those materials and by-products generated from, and commonly reused within, an original manufacturing process.
b) “Post-consumer Material” shall be defined as any material or finished product that has served its intended use and has been discarded for disposal or recovery having completed its life as a consumer item. “Post-consumer material” is included in the broader category of “Recovered Material”.
c) “Pre-consumer Material” shall be defined as any material or by-product generated after the manufacture of a product but before the product reaches the consumer, such as damaged or obsolete products. Pre-consumer Material does not include mill and manufacturing trim, scrap, or broken material that is generated at a manufacturing site and commonly reused on-site in the same or another manufacturing process.
d) "Recycled Product" shall be defined as a product that contains the highest amount of post-consumer material practicable, or when post-consumer material is impracticable for a specific type of product, contains substantial amounts of Pre-consumer Material.
e) "Recyclable Product" shall be defined as the ability of a product and its packaging to be reused, reconditioned for use, or recycled through existing recycling collection programs.
f) "Waste Reducing Product" shall be defined as any product that will result in less waste generated due to its use rather than another product designed to serve the same function with an greater waste generation rate. This shall include, but not be limited to, those products that can be reused, refilled or have a longer life expectancy and contain a lesser amount of toxic constituents.

6) PROPOSAL SUBMISSION REQUIREMENTS

In order to expedite the evaluation of proposals, the Proposer's response to this RFP shall follow the format and order of items, using the same paragraph identifiers, as set forth below.

a) Letter of Transmittal

The Proposer shall submit a letter on its letterhead, signed by an authorized representative, stating its experience and qualifications in meeting the requirements of this RFP. This letter shall include a statement on whether the Proposer is submitting a proposal as a single entity, a joint venture, or is partnering with another firm in a prime/subcontracting relationship. In all cases, information required for a single entity is required for each participant in a joint venture.

The Letter of Transmittal shall contain:

i) Name and address of the Proposer and an original signature on the Letter of Transmittal by an authorized representative on behalf of the Proposer;

ii) Name(s), title(s) and telephone number(s) of the individual(s) who are authorize to negotiate and execute the Contract;

iii) Name, title and telephone number of a contact person to which the Port Authority can address questions or issues related to this RFP;

iv) Name and address of proposed subcontractors, if any;

v) If a corporation: (a) a statement of the names and residences of its officers, and (b) a copy of its Certificate of Incorporation, with a written declaration signed by the secretary of the corporation, with the corporate seal affixed thereto, that the copy furnished is a true copy of the Certificate of Incorporation as of the date of the opening of the Proposals;

If a partnership: a statement of the names and residences of its principal officers, indicating which are general and which are special partners;

If an individual: a statement of residence;

If a joint venture: information on each of the parties consistent with the information requested above; if the Contract is awarded to a common law joint venture (a business enterprise formed by two or more companies) each member will be jointly and severally liable under the Contract.

b) Executive Summary

The Proposer shall submit a summary presenting the major features of its proposal and how the proposal satisfies the requirements contained in this RFP, as well as the special competencies and expertise of the Proposer to meet the requirements of this RFP.

c) Agreement on Terms of Discussion

The Proposer shall submit a copy of the "Agreement on Terms of Discussion," signed by an authorized representative of the Proposer. The Agreement format is included as Attachment A and shall be submitted by the Proposer without any alterations or deviations. Any Proposer who fails to sign the Port Authority's "Agreement on Terms of Discussion" will not have its proposal reviewed. If the Proposer is a joint venture, an authorized representative of each party must sign the Agreement.

d) Certifications With Respect to the Contractor's Integrity Provisions

The Proposer, by signing the Letter of Transmittal, makes the certifications in the "Contractor's Integrity Provisions," included as Section 37, Attachment B, General Contract Provisions of this RFP. If the Proposer cannot make any such certifications, it shall enclose an explanation of that inability.

e) Documentation of Proposer Prerequisites

The Proposer shall submit documentation to demonstrate that it meets all prerequisites, if any, included herein.

f) Proposal

The Proposer must submit a proposal that details and clearly describes its experience and capability to perform the work described in this RFP, its approach to such work and the cost of such work to the Port Authority. At a minimum, the proposal shall address the following:

i) Technical Plan & Work Approach:

The Proposer shall describe in detail its plan to, and its demonstrated ability to provide the required services described in the Scope of Work (Attachment D) and Functional Specifications (Attachment E). This includes the completeness of the services proposed; the ability to satisfy or exceed the requirements of the Service Level Agreements; the quality of management and the technical approach and resources to be used to assure consistently high-quality services; and the ability to provide the Port Authority with maximum flexibility in terms of services provided.

The Plan shall include, at minimum, the following:

(1) A detailed description of the Proposer's experience in maintaining, implementing, upgrading and using Parking Access and Revenue Control Systems, specifically as it pertains to transitioning from an old PARCS to a new PARCS at multiple sites while maintaining operational integrity and transaction processing capability.

(2) A detailed description of the Proposer's ability to complete the services proposed, specifically the Proposer's ability to deliver high-quality, onsite PARCS support services as required under the Service Level Agreements and while transitioning from an old PARCS to a new PARCS.

(3) A detailed Transition and Installation Plan, including Gantt charts, that illustrate the start and finish dates of the removal of old PARCS system, and the transition to and installation, acceptance testing and commissioning of a new PARCS system, including parking guidance subsystems, and parking reservation, prebooking and yield management capabilities. This plan should illustrate these elements by parking structure, by individual airport and as a total system.

(4) A documented methodology for the activities described in the Scope of Work herein. The methodology shall include mechanisms for improving the performance of said activities. The Proposer shall also describe its PARCS transition methodology and how, if at all, the transition would impact existing parking operations to maintain the overall integrity and operability of the PARCS and airport parking structures undergoing a PARCS transition.

(5) A detailed plan describing how the Proposer will maintain the uptime and functionality of the Existing PARCS system in light of the current vendor's discontinuance of its PARCS business and the anticipated scarcity of spare parts and hardware until the New PARCS is installed, accepted and commissioned.

(6) A documented application maintenance management methodology for recording changes made, new programs, documenting fixes and updates made to the application or underlying software, managing the development/production environment, putting new applications or new software into production and keeping users of the application and/or software informed.

(7) Identification of the processes and/or tools that will be used to measure performance against the Service Level Agreements stipulated in Section 14 of the Scope of Work (Attachment D).

(8) Identification of any tools, such as a "dashboard portal," that would enable the Authority to monitor service level requirements online or in real-time.

(9) Functionality and methods of generating custom reports.

(10) All security features, policies and practices for the System.

(11) Sample reports that will be provided.

(12) Detailed description of the services that will be provided.

(13) The extent to which the Proposer, and the managerial and supervisory personnel proposed to be dedicated to the Contract have the technical expertise and experience in implementing and managing similar services in a similar environment using the staff comparable in size to that necessary for the services to be provided here under, the anticipated function of each person on the Contract, a summary of the relevant experience of each person. The resumes of the individuals who are being recommended for these positions should be included in the Proposal.

(14) Experience of Proposer's senior management team in managing employees and conducting employee management programs, including, but not limited to:
(a) Staffing Plan
(b) Contract Management
(c) Proposed Maintenance Plan

(15) The Proposer shall submit a listing of all contracts involving the development, installation, management, testing and operation of PARCS that were performed by or are currently being performed by the Proposer within the last (3) years. For each Contract list at a minimum:
(a) The name and address of the Contracting Party
(b) The locations where the work was performed
(c) Duration of the Contract (commencement date and ending date)
(d) The approximate dollar amount of the Contract

(16) A description of the Proposer's quality assurance program to ensure that all work is performed in accordance with the Contract's requirements, including but not limited to the Audit Control Requirements Contract Checklist (Attachment J), Technology Standards for the Port Authority (Attachment K) and Information Security Handbook, October 15, 2008, Corrected as of February 9, 2009 (http://www.panynj.gov/business-opportunities/pdf/Corporate-Information-Security-Handbook.pdf or Attachment O);

NOTE: Company brochures alone shall not be submitted for the purpose of demonstrating experience and technical expertise. Submittals should be tailored to the specific requirements of this section.

ii) Cost Proposal

The degree to which the services and product required by this RFP are cost effective to the Authority and the overall cost of the proposed services and product. The Proposer shall submit a Cost Proposal indicating the compensation that it expects to receive. The Cost Proposal shall be complete and inclusive of all work required by this RFP and shall include, but not be limited to: capital work and installation costs, equipment removal and transition costs, monthly maintenance costs, material and labor costs, fuel costs, any salaries, health benefits and other benefits, overheads, profits, etc. The Cost Proposal should be submitted on Attachment C2 (Cost Proposal).

iii) Management/Firm Experience and Qualifications Approach

This plan details the Proposer's staffing capacity, financial stability, industry track record, and capability of managerial, technical and physical resources to deliver the required services over an extended period of time. This includes the level of staff experience and knowledge of the technology needed to support the Authority's current Parking Access and Revenue Control System (PARCS) and new PARCS to be provided hereunder; the Proposer's commitment to provide the requested services, to meet or exceed all requirements, and to develop and maintain a business alliance based on proposal and prior contract experience; the quality and effectiveness of the Proposer's MBE/WBE Plan and the extent to which it meets or exceeds MBE/WBE subcontracting provisions; and the Proposer's ability to mitigate and eliminate business risk.

The Proposer shall submit a Staffing Plan demonstrating a sufficient level of staffing experienced in the services needed to support the Scope of Work. At minimum, the Staffing Plan shall:

(1) The firm shall provide a complete description of how it intends to staff, implement and manage the required services hereunder, including any information that it believes would be helpful to the Port Authority in assessing its management approach and ability to provide the services.

(2) Clearly describe in detail your management philosophy and your approach to performance of the subject services, which shall include, but is not limited to, the following:

(a) An organization chart for this project that identifies the relationship between the Project Manager, Principals and other key individuals. Include their titles, office address, function, task responsibility and overall reporting relationships.

(b) A profile of each person identified in the organization chart that describes how his or her experience and technical capabilities will assist in the successful performance and completion of the Contract. Include the number and relevant experience of all managerial and supervisory personnel proposed to be dedicated to the Contract.

(c) Approach to keeping the Authority informed of any issues and progress during performance of the contemplated services.

(d) Approach to quality control/quality assurance in terms of both technical review and compliance with the overall Contract and schedule requirements.

(3) Provide a statement indicating the qualifications and relevant experience of managerial and supervisory personnel employed by the firm who are to be exclusively dedicated to the Contract, including:

(a) Their length of service with the firm
(b) The anticipated function of each person on the Contract
(c) A summary of the relevant experience of each person listed
(d) The resumes of the individuals who are being recommended for these positions should be included in the submission.

(4) Submit proposed labor, supervisory, on-site management and work plans.

(5) The Proposer shall provide a plan in handling emergency situations and the proposed emergency procedures to identify and handle potential emergency situations such as, but not limited to: inclement weather, power outages and interruptions in transportation infrastructure to and from the facilities, etc.

(6) The Proposer's training and safe work environment plans for this Contract;

(7) Contractor's audit program;

(8) MBE/WBE participation plan;

(9) Certification of Environmentally Preferable Products/ Practices;

(10) The Proposer shall provide documentation relevant to establish the Proposer's capability to meet all terms and conditions set forth herein, including insurance requirements.

(11) Include a description of the Proposer's experience in the applications and products proposed and specified herein.

(12) Specify the minimum technical expertise and certifications of assigned staff in administration, support, maintenance and repair of PARCS systems;

(13) Include a statement documenting the amount of staff that will be dedicated to performing the Contract;

(14) Describe how the Proposer intends to provide staffing coverage needed to satisfy the Service Level Agreement and the Port Authority's operational needs at John F. Kennedy International Airport, Newark Liberty International Airport, LaGuardia Airport and Stewart International Airport;

(15) Indicate the amount and exact location of sites that will be utilized in managing the Contract, including any sites located outside of the Continental United States;

(16) Indicate the tasks to be performed at each identified site, and the tasks to be performed at the Port Authority airports specified in (e) above;

(17) Indicate the staffing, by specialty, at each site and their level of experience and length of employment;

(18) Describe the composition of the Proposer's regional offices;

(19) Describe in detail the Proposer's intended organizational and operational structure to be employed for Contract management. This section shall include or indicate:

(a) Proposer's principal personnel and their qualifications, experience and length of employment;
(b) Resumes and any other information that will demonstrate the experience and qualifications of the Proposer's staff (and, if applicable, that of its subcontractors), including the qualifications, experience, and certifications of its technical management and key technical staff who will participate in fulfilling the requirements of the submitted proposal;
(c) The qualifications and resume of the individual(s) who will function as the Proposer's Account Manager for the Contract;
(d) A proposed Organizational Chart for the Contract, which shall indicate key supervisory personnel to be assigned for the duration of the Contract and their anticipated functions and relevant experience;
(e) The Proposer's escalation procedure and all contact information;

(20) Specify any assumptions regarding Authority-provided offices, office equipment and other workspace requirements and equipment the Authority is expected to provide the Proposer's staff. The Proposer's Staffing Plan shall consider the geographic dispersion of facilities and the Service Levels required by the Contract.

(21) Include a statement of the total amount of full-time (minimum of forty [40] hours per week) employees currently employed by the Proposer and deployed in similar engagements, and the number employed in each of the preceding five (5) years. The statement shall also identify the amount and experience of its staff.

(22) Indicate the sources (e.g. subcontractors, etc.), if any, that the Proposer will utilize to staff the functions required for this Contract. The Proposer shall state whether such sources have provided such services on similar projects for the Proposer or other firms, and include a list indicating specific contracts and describing the business relationship utilized to provide such services, the past experience of key personnel and their length of service with the firm, and their functions and responsibilities.

(23) Include a Contractor Identity Check/Background Screening Plan, which demonstrates how the Proposer will ensure that only employees who were successfully prescreened and properly credentialed perform the services herein. This Plan shall be applicable to all years of the Contract and shall include the length of time researched for the identity check/background screening on new hires, which shall be at a minimum of 10 years of employment history or verification of what an employee documented they have done in the last 10 years preceding the date of the investigation, resources utilized to perform this, and the frequency at which it is performed on current employees.

iv) Contractor Identity Check/Background Screening Plan

The Proposer shall submit a Contractor Identity Check/Background Screening Plan, which demonstrates how the Proposer will ensure that only employees who were successfully prescreened and properly credentialed perform the services herein. This Plan shall be applicable to all years of the Contract and shall include, but not be limited to, the following:
The length of time researched for the identity check/background screening on new hires, which shall be at a minimum of 10 years of employment history or verification of what an employee documented they have done in the last 10 years preceding the date of the investigation, resources utilized to perform this, and the frequency at which it is performed on current employees.

v) Business Risk

The Proposer shall submit risk assessment and succession plans to the Contractor and the Port Authority, that assess the business risk in taking on the significant amount of new work that will be required under this Contract. The risk assessment plan should take into account all work currently under contract, as well as work that is under contract to companies, which the Proposer owns, controls or has an interest.

The Proposer shall provide any other information that is related to the requirements in this Section (Section E), that the Proposer believes would be helpful to the Port Authority in the evaluation of its proposal.

vi) License Agreement

The proposer shall include with its submission copies of standard software license agreements, including as applicable, whether it plans to use open-source or open-source based software and how it will comply with open-source license requirements, that the Proposer would reasonably expect the Authority to execute as part of this agreement. Request for this information does not signify the Authority's acceptance or agreement to enter in any such license or other agreement.

g) Acknowledgement of Addenda

If any Addenda are posted or sent as part of this RFP, the Proposer shall complete, sign and include with its Proposal the addenda form(s). In the event any Proposer fails to conform to these instructions, its proposal will nevertheless be construed as though the Addenda had been acknowledged.

If the Proposer downloaded this RFP document, it is the responsibility of the Proposer to periodically check the Port Authority website at http://www.panynj.gov/business-opportunities/bid-proposal-advertisements.html and download any addenda that might have been issued in connection with this solicitation.

h) Acceptance of Standard Contract Terms and Conditions

The Port Authority has attached to this RFP as Attachment B, General Contract Provisions governing the Contract. The Proposer is expected to agree with these General Contract Provisions. However, if the Proposer has any specific exceptions, such exceptions should be set forth in a separate letter included with its response to this RFP. After the proposal due date, the Proposer will be precluded from raising any exceptions unless such exceptions are justified by and directly related to substantive changes in the business or technical requirements and are agreed to by the Proposer and the Port Authority. The Port Authority is under no obligation to accept or consider exceptions or

changes suggested by any proposer.

i) MBE/WBE Plan

The Proposer shall submit an MBE/WBE Plan in accordance with the MBE/WBE Subcontracting Provisions hereunder.

j) Checklist of Features or Requirements

The Proposer shall complete and submit the Checklist of Features or Requirements attached to this RFP (Attachment P).

7) CONDITIONS FOR THE SUBMISSION OF A PROPOSAL

In addition to all other requirements of this RFP, the Proposer agrees to the following conditions for the submission of its proposal.

a) Changes to this RFP

At any time, in its sole discretion, the Port Authority may by written addenda, modify, correct, amend, cancel and/or reissue this RFP. If an addendum is issued prior to the date proposals are due, it will be provided to all parties in the medium in which the parties obtained the RFP. If an addendum is issued after proposals have been received, the addendum will be provided only to those whose proposals remain under consideration at such time.

b) Proposal Preparation Costs

The Port Authority shall not be liable for any costs incurred by the Proposer in the preparation, submittal, presentation, or revision of its proposal, or in any other aspect of the Proposer's pre-contract activity. No Proposer is entitled to any compensation except under an agreement for performance of services signed by an authorized representative of the Port Authority and the Proposer.

c) Disclosure of Proposal Contents / Use of Ideas and Materials

Proposal information is not generally considered confidential or proprietary. All information contained in the proposal is subject to the "Agreement on Terms of Discussion" attached hereto as Attachment A.

d) Ownership of Submitted Materials

All materials submitted in response to or in connection with this RFP shall become the property of the Port Authority. Selection or rejection of a Proposal shall not affect this right.

e) Subcontractors

If a Proposer intends to use subcontractor(s) the Proposer must identify in its proposal the names of the subcontractor(s) and the portions of the work the subcontractor(s) will perform.

f) Conflict of Interest

If the Proposer or any employee, agent or subcontractor of the Proposer may have a possible conflict of interest, or may give the appearance of a possible conflict of interest, the Proposer shall include in its proposal a statement indicating the nature of the conflict. The Port Authority reserves the right to disqualify the Proposer if, in its sole discretion, any interest disclosed from any source could create a conflict of interest or give the appearance of a conflict of interest. The Port Authority's determination regarding any questions of conflict of interest shall be final.

g) Authorized Signature

Proposals must be signed by an authorized corporate officer (e.g., President or Vice President), General Partner, or such other individual authorized to bind the Proposer to the provisions of its proposal and this RFP.

h) References

The Port Authority may consult any reference familiar with the Proposer regarding its current or prior operations and projects, financial resources, reputation, performance, or other matters. Submission of a proposal shall constitute permission by the Proposer for the Port Authority to make such inquiries and authorization to third parties to respond thereto.

i) Evaluation Procedures and Negotiation

Only Proposers which meet the prerequisites, if any, may have their proposals evaluated based on the evaluation criteria set forth in this RFP. The Port Authority may use such procedures that it deems appropriate to evaluate such proposals. The Port Authority may elect to initiate contract negotiations with one or more Proposers including negotiation of costs/price(s) and any other term or condition, including modifying any requirement of this RFP. The option of whether or not to initiate contract negotiations rests solely with the Port Authority.

j) Most Advantageous Proposal/No Obligation to Award

The Port Authority reserves the right to award the Contract to other than the Proposer proposing the lowest price. The Contract will be awarded to the Proposer whose proposal the Port Authority believes, in its sole discretion, will be the most advantageous to the Port Authority. Neither the release of this RFP nor the acceptance of any response thereto shall compel the Port Authority to accept any proposal. The Port Authority shall not be obligated in any manner whatsoever to any Proposer until a proposal is accepted by the Port Authority in the manner provided in the Section of this RFP entitled "Proposal Acceptance or Rejection."

k) Multiple Contract Awards

The Port Authority reserves the right to award multiple Contracts for the products, work and/or services that are the subject matter of this RFP and Proposers are hereby given notice that they may not be the Port Authority's only contractor for such products, work and/or services.

l) Right to Extend Contract

If this is a proposal for a contract for a term of years, including specified options for renewal, the Port Authority reserves the additional right to extend the contract term for an additional 180 days, upon the same terms and conditions of the original Contract negotiated between the Port Authority and the successful Proposer.

m) Rights of the Port Authority

i) The Port Authority reserves all its rights at law and equity with respect to this RFP including, but not limited to, the unqualified right, at any time and in its sole discretion, to change or modify this RFP, to reject any and all proposals, to waive defects or irregularities in proposals received, to seek clarification of proposals, to request additional information, to request any or all Proposers to make a presentation, to undertake discussions and modifications with one or more Proposers, or to negotiate an agreement with any Proposer or third person who, at any time, subsequent to the deadline for submissions to this RFP, may express an interest in the subject matter hereof, to terminate further participation in the proposal process by a Proposer or to proceed with any proposal or modified proposal, which in its judgment will, under all circumstances, best serve the Port Authority's interest. The Port Authority may, but shall not be obliged to, consider incomplete proposals or to request or accept additional material or information. The holding of any discussions with any Proposer shall not constitute acceptance of a proposal, and a proposal may be accepted with or without discussions.

ii) No Proposer shall have any rights against the Port Authority arising from the contents of this RFP, the receipt of proposals, or the incorporation in or rejection of information contained in any proposal or in any other document. The Port Authority makes no representations, warranties, or guarantees that the information contained herein, or in any addenda hereto, is accurate, complete, or timely or that such information accurately represents the conditions that would be encountered during the performance of the contract. The furnishing of such information by the Port Authority shall not create or be deemed to create any obligation or liability upon it for any reason whatsoever and each Proposer, by submitting its proposal, expressly agrees that it has not relied upon the foregoing information, and that it shall not hold the Port Authority liable or responsible therefor in any manner whatsoever. Accordingly, nothing contained herein and no representation, statement or promise, of the Port Authority, its directors, officers, agents, representatives, or employees, oral or in writing, shall impair or limit the effect of the warranties of the Proposer required by this RFP or Contract and the Proposer agrees that it shall not hold the Port Authority liable or responsible therefor in any manner whatsoever.

iii) At any time and from time to time after the opening of the proposals, the Port Authority may give oral or written notice to one or more Proposers to furnish additional information relating to its proposal and/or qualifications to perform the services contained in this RFP, or to meet with designated representatives of the Port Authority. The giving of such notice shall not be construed as an acceptance of a proposal. Information shall be submitted within three (3) calendar days after the Port Authority's request unless a shorter or longer time is specified therein.

n) No Personal Liability

Neither the Commissioners of the Port Authority, nor any of them, nor any officer, agent or employee thereof shall be charged personally with any liability by a Proposer or another or held liable to a Proposer or another under any term or provision of this RFP or any statements made herein or because of the submission or attempted submission of a proposal or other response hereto or otherwise.

8) ATTACHMENTS

Attachment A	Agreement on Terms of Discussion
Attachment B	General Contract Terms and Conditions
Attachment C1	Contract Specific Terms and Conditions
Attachment C2	Pricing Sheets
Attachment D	Scope of Work
Attachment E	Functional Specifications
Attachment F	Proposer Reference Form
Attachment G	MBE/WBE Subcontracting Plan
Attachment H	Certified Environmentally Preferable Products/Practices Form

Attachment I	Background of Existing System
Attachment J	Audit Controls Requirement Contract Checklist
Attachment K	Technology Standards for the Port Authority
Attachment L	Computing Resources Guidelines
Attachment M	Cyber Security Guidelines for the Port Authority of New York and New Jersey
Attachment N	Escrow Agreement
Attachment O	Information Security Handbook
Attachment P	Submittal Requirements
Attachment Q	Change Control Example
Attachment R	Existing System Preventative Maintenance
Attachment S	Spare Parts Inventory
Attachment T	*E-ZPass®* ACH Requirement
Attachment U	*E-ZPass®* Interface File and Reporting Specifications
Attachment V	Non Disclosure Agreement
Attachment W	Cloud Computing Framework
Attachment X	Qualification Requirements

Parking Access and Revenue Control System—Design, Installation & Maintenance

Attachment A
Agreement on Terms of Discussion

AGREEMENT ON TERMS OF DISCUSSION

The Port Authority's receipt or discussion of any information (including information contained in any proposal, vendor qualification(s), ideas, models, drawings, or other material communicated or exhibited by us or on our behalf) shall not impose any obligations whatsoever on the Port Authority or entitle us to any compensation therefor (except to the extent specifically provided in such written agreement, if any, as may be entered into between the Port Authority and us). Any such information given to the Port Authority before, with or after this Agreement on Terms of Discussion ("Agreement"), either orally or in writing, is not given in confidence. Such information may be used, or disclosed to others, for any purpose at any time without obligation or compensation and without liability of any kind whatsoever. Any statement which is inconsistent with this Agreement, whether made as part of or in connection with this Agreement, shall be void and of no effect. This Agreement is not intended, however, to grant to the Port Authority rights to any matter, which is the subject of valid existing or potential letters patent.

Any information (including information contained in any proposal, vendor qualification(s), ideas, models, drawings, or other material communicated or exhibited by us or on our behalf) provided in connection with this procurement is subject to the provisions of the Port Authority Freedom of Information Code and Procedure adopted by the Port Authority's Board of Commissioners on October 22, 2014, which may be found on the Port Authority website at: http://www.panynj.gov/corporate-information/pdf/foi-code.pdf. The foregoing applies to any information, whether or not given at the invitation of the Authority.

_____
(Company)

_____
(Signature)

_____
(Title)

_____
(Date)

ORIGINAL AND PHOTOCOPIES OF THIS PAGE ONLY.
DO NOT RETYPE.

Parking Access and Revenue Control System—Design, Installation & Maintenance

Attachment B
General Contract Provision

1) GENERAL AGREEMENT

The undersigned (hereinafter referred to as the "Contractor" or “you”) agrees to provide, and The Port Authority of New York and New Jersey (hereinafter referred to as the "Authority") agrees to accept to provide all the necessary supervision, personnel, equipment, materials and all other things necessary to perform the Services required by this Contract as more fully set forth in the Scope of Work attached hereto and made a part hereof. The Scope of Work requires the doing of all things necessary or proper for or incidental to the requirements as set forth in the Scope of Work. All things not expressly mentioned in the Scope of Work but involved in carrying out their intent are required by the Scope of Work and the Contractor shall perform the same as though they were specifically mentioned, described and delineated.

2) DEFINITIONS

To avoid undue repetition, the following terms, as used in this Agreement, shall be construed as follows:

Authority or Port Authority - means the Port Authority of New York and New Jersey.

Contract, Document or Agreement - mean the writings setting forth the scope, terms, conditions and Specifications for the procurement of Goods and/or Services, as defined hereunder and shall include, but not be limited to: Request for Proposal (RFP), Purchase Order (PO), Cover Sheet, executed Signature Sheet, AND PRICING SHEETS with Contract prices inserted," "STANDARD CONTRACT TERMS AND CONDITIONS," and, if included, attachments, endorsements, schedules, exhibits, or drawings, the Authority's acceptance and any written addenda issued over the name of the Assistant Director, Commodities and Services Division, Procurement Department.

Days or Calendar Days - mean consecutive calendar days, Saturdays, Sundays, and holidays, included.

Director - means the Director of the Department which operates the facility of the Port Authority at which the services hereunder are to be performed, for the time being, or his/her successor in duties for the purpose of this Contract, or one of his/her authorized representatives for the purpose of this Contract.

Facility- Port Authority Facilities within the Port District, as set forth in Attachment C: “Port Authority Facilities”.

Project Manager (or Manager) - means the individual with day-to-day responsibility for managing the project on behalf of the Port Authority.

No person shall be deemed a representative of the Director or Manager except to the extent specifically authorized in an express written notice to the Contractor signed by the Director or Manager, as the case may be. Further, no person shall be deemed a successor in duties of the Director unless the Contractor is so notified in writing signed by the Assistant Director, Commodities & Services Division, Procurement Department. No person shall be deemed a successor in duties of the Manager unless the Contractor is so notified in a writing signed by the Director.

Services or Work - mean all services, equipment and materials (including materials and equipment, if any, furnished by the Authority) and other facilities and all other things necessary or proper for, or incidental to the services to be performed or goods to be furnished in connection with the service to be provided hereunder, as set forth in the Scope of Work.

Specifications- mean all requirements of this RFP, technical and otherwise, for the performance of the Scope of Work and services hereunder.

Holidays: The following legal holidays will be observed at Port Authority offices and facilities:

New Year's Day	Columbus Day
Martin Luther King, Jr. Day	Veteran's Day
Presidents Day	Thanksgiving Day
Memorial Day	Day After Thanksgiving
Independence Day	Christmas Day
Labor Day	

Do not perform any Work unless authorized by the Authority on these days.

Minority Business Enterprise (MBE) - means a business entity which is at least fifty-one percent (51%) owned and controlled by one or more members of one or more minority groups, or, in the case of a publicly held corporation, at least fifty-one percent (51%) of the stock of which is owned by one or more minority groups, and whose management and daily business operations are controlled by one or more such individuals who are citizens or permanent resident aliens.

"Minority Group" means any of the following racial or ethnic groups:

a) Black persons having origins in any of the Black African racial groups not of Hispanic origin;
b) Hispanic persons of Mexican, Puerto Rican, Dominican, Cuban, Central or South American culture or origin, regardless of race;
c) Asian and Pacific Islander persons having origins in any of the original peoples of the Far East, Southeast Asia, The Indian Subcontinent, or the Pacific Islands;

d) Native American or Alaskan native persons having origins in any of the original peoples of North America and maintaining identifiable tribal affiliations through membership and participation or community identification.

Month - unless otherwise specified, means a calendar month.

Site of the Work - or words of similar import shall mean the Facility and all buildings and properties associated therewith as described in this Contract.

Small Business Enterprise (SBE) - The criteria for a Small Business Enterprise are:
a) The principal place of business must be located in New York or New Jersey;
b) The firm must have been in business for at least three years with activity;
c) Average gross income limitations by industry as established by the Port Authority.

Subcontractor - mean anyone who performs work (other than or in addition to the furnishing of materials, plant or equipment) in connection with the services to be provided hereunder, directly or indirectly for or on behalf of the Contractor (and whether or not in privity of contract with the Contractor), but shall not include any person who furnished merely his own personal labor or his own personal services. "Subcontractor", however, shall exclude the Contractor or any subsidiary or parent of the Contractor or any person, firm or corporation which has a substantial interest in the Contractor or in which the Contractor or the parent or the subsidiary of the Contractor, or an officer or principal of the Contractor or of the parent of the subsidiary of the Contractor has a substantial interest, provided, however, that for the purpose of the clause hereof entitled "Assignments and Subcontracts" the exclusion in this paragraph shall not apply to anyone but the Contractor itself.

Week - unless otherwise specified, means seven (7) consecutive calendar days, Saturdays, Sundays, and holidays.

Woman-owned Business Enterprise (WBE) - shall mean a business enterprise which is at least fifty-one percent (51%) owned by one or more women, or, in the case of a publicly held corporation, at least fifty-one percent (51%) of the stock of which is owned by one or more women and whose management and daily business operations are controlled by one or more women who are citizens or permanent or resident aliens.

Work Day- unless otherwise specified, means a day between Monday and Friday with Monday and Friday included.

3) GENERAL PROVISIONS

a) Under no circumstances shall you or your subcontractors communicate in any way with any department, board, agency, commission, or other organization or any person whether governmental or private in connection with the services to be performed

hereunder except upon prior written approval and instructions of the Director, provided, however, that data from manufacturers and suppliers of materials, devices and equipment shall be obtained by you when you find such data necessary unless otherwise instructed by the Authority.

b) Any services performed for the benefit of the Authority at any time by you or on your behalf, even if expressly and duly authorized by the Authority, shall be deemed to be rendered under and subject to this Agreement (unless referable to another expressly written, duly executed agreement by the same parties), whether such additional services are performed prior to, during or subsequent to the services described herein, and no rights or obligations shall arise out of such additional services except as provided under this Agreement.

c) The Contractor shall observe and obey (and compel its officers, employees, guests, invitees, and those doing business with it, to observe and obey) the rules and regulations of the Port Authority now in effect, and such further rules and regulations which may from time to time during the effective period of this Contract, be promulgated by the Port Authority for reasons of safety, health, preservation of property, or maintenance of a good and orderly appearance of the Facilities, or for the safe and efficient operation of the Facilities. The Port Authority agrees that, except in cases of emergency, it shall give notice to the Contractor of every rule and regulation hereafter adopted by it.

d) This Contract does not constitute the Contractor as an agent or representative of the Port Authority for any purpose whatsoever. The Contractor shall perform all services hereunder as an independent Contractor and the Contractor, its officers, and employees shall not be deemed to be agents, servants, or employees of the Port Authority.

4) INTELLECTUAL PROPERTY

a) Except as provided below: as between the Port Authority and the Contractor all process flows, codes including, but not limited to scripts, programs, routines, processes, procedures, documentation, estimates, reports, records, data, charts, documents, models, designs, renderings, drawings, specifications, photographs, computations, computer tapes or discs, and other documentation of any type whatsoever, whether electronic or in the form of writing, figures or delineations, which are prepared or compiled in connection with this Agreement, shall become the exclusive property of the Authority, and the Authority shall have the exclusive right to use or permit the use of them and any ideas or methods represented by them for any purpose and at any time without other compensation than that specifically provided for herein. With regard to training manuals or any other knowledge transfer documentation, communication or presentation prepared under this Agreement the Authority shall expressly have the right to use, alter and reproduce including electronically, said manuals for its internal business purposes. The Contractor hereby warrants and represents that the Authority

will have at all times the ownership and rights provided for in the immediately preceding sentence free and clear of all claims of third persons whether presently existing or arising in the future and whether presently known to either of the parties to this Agreement or not. Any information given to the Port Authority before, with or after submission of the Agreement on Terms of Discussion, either orally or in writing, is not given in confidence and may be used, or disclosed to others, for any purpose at any time without obligation or compensation and without liability of any kind whatsoever except as otherwise set forth in the Agreement On Terms Of Discussion.

The right to use all patented materials, appliances, processes of manufacture or types of construction, trade and service marks, copyrights and trade secrets, collectively hereinafter referred to as "Intellectual Property Rights", in the performance of the work, shall be obtained by the Contractor without separate or additional compensation. Where the services under this Agreement require the Contractor to provide materials, equipment or software for the use of the Port Authority or its employees or agents, the Port Authority shall be provided with the Intellectual Property Rights required for such use without further compensation than is provided for under this Agreement.

b) All preexisting information or documentation including computer programs or code including source code, of the Contractor, utilized by the Contractor hereunder in the performance of his services hereunder shall be deemed licensed to the Authority for the duration and purposes of this agreement, but shall remain the property of the Contractor.

c) When in the performance of the contract services the Contractor utilizes passwords or codes for any purpose, at any time during or after the performance of such services, upon written request by the Authority, the Contractor shall make available to the designated Authority representative all such passwords and codes.

d) Third party software not specially prepared for the purpose of this agreement but utilized by the Contractor hereunder in the performance of his services hereunder shall be licensed to the Contractor and the Authority for the duration and purposes of this agreement but shall remain the property of said third party.

e) The above-described software shall be furnished by the Contractor without additional compensation.

5) PROPRIETARY RIGHTS IN SUBJECT MATTER NOT WITHIN THE INTELLECTUAL PROPERTY CLAUSE

If in accordance with this Contract the Contractor furnishes research, development or consultative services in connection with the performance of the Work and if in the course of such research, development, or consultation patentable or copyrightable subject matter or trade secrets or other proprietary matter is produced by the Contractor, its officers, agents,

employees, subcontractors, or suppliers, not custom software, and not covered under clause 6 entitled Intellectual Property, the Authority shall have, without cost or expense to it, an irrevocable, non-exclusive, royalty-free license to make, have made, and use, either itself or by anyone on its behalf, such subject matter in connection with any activity now or hereafter engaged in or permitted by the Authority. Promptly upon request by the Authority, the Contractor shall furnish or obtain from the appropriate person a form of license satisfactory to the Authority, but it is expressly understood and agreed that as between the Contractor and the Authority the license herein provided for shall nevertheless arise for the benefit of the Authority immediately upon the production of said subject matter and shall not await formal exemplification in a written license agreement as provided for above. Such license may be transferred by the Authority to its successors, immediate or otherwise, in the operations of or ownership of any facility now or hereafter operated by the Authority or the Authority but such license shall not be otherwise transferable.

The right of the Authority as well as the Contractor to use all patented material, compositions of matter, manufactures, apparatus, appliances, processes of manufacture or types of construction as well as any copyrightable matter, trade secrets or other proprietary matters, shall be obtained by the Contractor without separate or additional compensation whether the same is patented or copyrighted before, during or after the performance of the Work.

6) INDEMNITY IN REGARD TO INFRINGEMENT MATTER

The Contractor shall indemnify the Authority against and save it harmless from all loss and expense incurred in the defense, settlement or satisfaction of any claims in the nature of patent, copyright, or other proprietary rights infringement arising out of or in connection with the Authority's use, in accordance with the preceding clause of such patentable subject matter or patented material, compositions of matter, manufactures, apparatus, appliances, processes of manufacture or types of construction, or copyrighted matter or other matter protected as intellectual property. If requested by the Authority and if notified promptly in writing of any such claims, the Contractor shall conduct all negotiations with respect to and defend such claim without expense to the Authority. If the Authority be enjoined from using any of the facilities which form the subject matter of this Contract, and as to which the Contractor is to indemnify the Authority against proprietary rights claims, the Authority may, at its option and without thereby limiting any other right it may have hereunder or at law or in equity, require the Contractor to supply, temporarily or permanently, facilities not subject to such injunction and not infringing any proprietary rights and if the Contractor shall fail to do so, the Contractor shall, at its expense, remove all such facilities and refund the cost thereof to the Authority and otherwise equitably adjust compensation and take such steps as may be necessary to ensure compliance by the Authority with such injunction, to the satisfaction of the Authority.

The Contractor shall promptly and fully inform the Director of any claims or disputes for infringement or otherwise, whether existing or potential, of which it has knowledge relating to any Intellectual Property used, developed or licensed in connection with the performance of the Work or otherwise in connection with this Contract.

7) CONTRACT RECORDS AND DOCUMENTS – PASSWORDS AND CODES

When the performance of the contract services requires the Contractor to produce, compile or maintain records, data, drawings, or documents of any kind, regardless of the media utilized, then all such records, drawings, data and documents which are produced, prepared or compiled in connection with this contract, shall become the property of the Port Authority, and the Port Authority shall have the right to use or permit the use of them and any ideas or methods represented by them for any purpose and at any time without other compensation than that specifically provided herein.

When in the performance of the contract services the Contractor utilizes passwords or codes for any purpose, at any time during or after the performance of such services, upon written request by the Authority, the Contractor shall make available to the designated Authority representative all such passwords and codes.

8) COMPLIANCE WITH WEB SITE TERMS OF USE AND PRIVACY POLICIES

Subject to all of the provisions of this Contract including, without limitation, the obligations of the Contractor under the section hereof entitled “Indemnification and Risks Assumed by the Contractor,” the Contractor shall, and shall compel its employees, agents and subcontractors, to strictly abide by and comply with the policies established by the Authority governing the use of the Authority’s web sites as set forth in the Authority web sites Terms of Use and Privacy Statement as the same may be supplemented or amended. The Contractor shall immediately implement all procedures in connection with such policies and in furtherance thereof as directed by the Authority.

9) TIME IS OF THE ESSENCE

The Contractor's obligations for the performance and completion of all work within the time or times provided for in this Contract are of the essence of this Contract.

10) FINAL PAYMENT

After satisfactory completion of all services required hereunder, and upon receipt from the Contractor of such information as may be required, the Director shall certify in writing to the Contractor the total compensation earned by the Contractor.

If so required, the Contractor shall thereupon furnish to the Authority a detailed sworn statement of all claims, just and unjust, of subcontractors, materialmen and other third

persons then outstanding which he has reason to believe may thereafter be made on account of the services provided under this Agreement.

Within thirty days after issuance of such certificate of total compensation earned (or within thirty days after receipt of the documents provided for in the immediately preceding paragraph, if required and if such date is later), the Port Authority shall pay to the Contractor by check the amount stated in said certificate, less all other payments and advances whatsoever to or for the account of the Contractor. All prior estimates and payments shall be subject to correction in this payment, which is throughout this Agreement called the Final Payment.

The acceptance by the Contractor, or by anyone claiming by or through him, of the Final Payment shall be and shall operate as a release to the Authority of all claims and of all liability to the Contractor for all things done or furnished in connection with this contract and for every act and neglect of the Authority and others relating to or arising out of the this contract, including claims arising out of breach of the contract and claims based on claims of third persons.

The Contractor's agreement as provided in the immediately preceding paragraph shall be deemed to be based upon the consideration forming part of this Contract as a whole and not to be gratuitous; but in any event even if deemed gratuitous and without consideration, such agreement as provided in the immediately preceding paragraph shall nevertheless be effective. Such release shall include all claims, whether or not in litigation and even though still under consideration by the Authority. Such release shall be effective notwithstanding any purported reservation of right by the Contractor to preserve such claim. The acceptance of any check designated as "Final Payment" or bearing any similar designation shall be conclusively presumed to demonstrate the intent of the Contractor that such payment was intended to be accepted as final, with the consequences provided in this numbered clause, notwithstanding any purported reservation of rights.

The Contractor agrees that he shall not be entitled to, and hereby waives any right he might otherwise have to, and shall not seek any judgment whether under this Contract or otherwise for any such Final Payment or for an amount equivalent thereto or based thereon, or for any part thereof, if such judgment would have the effect of varying, setting aside, disregarding or making inapplicable the terms of this numbered clause or have the effect in any way of entitling the Contractor to accept such Final Payment or an amount equivalent thereto or based thereon or any part thereof other than in the same fashion as a voluntary acceptance of a Final Payment subject to all the terms of this Contract including this numbered clause, unless and until the Contractor should obtain a judgment on any claim arising out of or in connection with this Contract (including a claim based on breach of contract) for an amount not included in said Final Payment.

11) DEFAULT, REVOCATION OR SUSPENSION OF CONTRACT

a) If one or more of the following events shall occur:
   i) If fire or other event shall destroy all or a substantial part of the Facility, asset or infrastructure necessary to perform the Scope of Work.
   ii) If any governmental agency shall condemn or take a temporary or permanent interest in all or a substantial part of the Facility, or all of a part of the Port Authority's interest herein;

   then upon the occurrence of such event or at any time thereafter during the continuance thereof, the Port Authority shall have the right on twenty-four (24) hours written notice to the Contractor to revoke this Contract, such revocation to be effective upon the date and time specified in such notice.

   In such event this Contract shall cease and expire on the effective date of revocation as if said date were the date of the expiration of this Contract. Such revocation shall not, however, relieve the Contractor of any liabilities or obligations hereunder which shall have accrued on or prior to the effective date of revocation.

b) If one or more of the following events shall occur:

   i) The Contractor shall become insolvent, or shall take the benefit of any present or future insolvency statute, or shall make a general assignment for the benefit of creditors, or file a voluntary petition in bankruptcy or a petition or answer seeking an arrangement or its reorganization or the readjustment of its indebtedness under the federal bankruptcy laws or under any other law or statute of the United States or of any State thereof, or consent to the appointment of a receiver, trustee, or liquidator of all or substantially all its property; or
   ii) By order or decree of a court the Contractor shall be adjudged bankrupt or an order shall be made approving a petition filed by any of the creditors, or, if the Contractor is a corporation, by any of the stockholders of the Contractor, seeking its reorganization or the readjustment of its indebtedness under the federal bankruptcy laws or under any law or statute of the United States or of any State thereof; or
   iii) A petition under any part of the federal bankruptcy laws or an action under any present or future insolvency law or statute shall be filed against the Contractor and shall not be dismissed within thirty (30) days after the filing thereof; or
   iv) The interest of the Contractor under this Contract shall be transferred to, passed to or devolve upon, by operation of law or otherwise, any other person, firm or corporation; or
   v) The Contractor, if a corporation, shall, without the prior written approval of the Port Authority, become a surviving or merged corporation in a merger, a constituent corporation in a consolidation, or a corporation in dissolution; or
   vi) If the Contractor is a partnership, and the said partnership shall be dissolved as the result of any act or omission of its copartners or any of them, or by operation of law or the order or decree of any court having jurisdiction, or for any other reason whatsoever; or

vii) By or pursuant to, or under authority of any legislative act, resolution or rule, or any order or decree of any court or governmental board, agency or officer having jurisdiction, a receiver, trustee, or liquidator shall take possession or control of all or substantially all of the property of the Contractor and such possession or control of all or substantially all of the property of the Contractor and shall continue in effect for a period of fifteen (15) days;

then upon the occurrence of any such event or at any time thereafter during the continuance thereof, the Port Authority shall have the right upon five (5) days notice to the Contractor to terminate this Contract and the rights of the Contractor hereunder; termination to be effective upon the date and time specified in such notice as if said date were the date of the expiration of this Contract. Termination shall not relieve the Contractor of any liabilities or obligations hereunder which have accrued on or prior to the effective date of termination.

c) If any of the following shall occur:

i) The Contractor shall cease, abandon any part of the service, desert, stop or discontinue its services in the premises for any reason whatsoever and regardless of the fault of the Contractor; or

ii) The Contractor shall fail to keep, perform and observe each and every other promise, covenant and agreement set forth in this Contract on its part to be kept, performed or observed, within five (5) days after receipt of notice of default thereunder from the Port Authority (except where fulfillment of its obligations requires activity over a greater period of time, and the Contractor shall have commenced to perform whatever may be required for fulfillment within five (5) days after receipt of notice and continues such performance without interruption except for causes beyond its control);

then upon the occurrence of any such event or during the continuance thereof, the Port Authority shall have the right on twenty four (24) hours notice to the Contractor to terminate this Contract and the rights of the Contractor hereunder, termination to be effective upon the date and time specified in such notice. Termination shall not relieve the Contractor of any liabilities, which shall have accrued on or prior to the effective date of termination.

d) If any of the events enumerated in this Section shall occur prior to commencement date of this Contract the Port Authority upon the occurrence of any such event or any time thereafter during the continuance thereof by twenty-four (24) hours notice may terminate or suspend this Contract and the rights of the Contractor hereunder, such termination or suspension to be effective upon the date specified in such notice.

e) No payment by the Port Authority of any monies to the Contractor for any period or periods after default of any of the terms, covenants or conditions hereof to be

performed, kept and observed by the Contractor and no act or thing done or omitted to be done by the Port Authority shall be deemed to be a waiver of the right of the Port Authority to terminate this Contract or of any other right or remedies to which the Port Authority may be entitled because of any breach thereof. No waiver by the Port Authority of any default on the part of the Contractor in the performance of any of the terms, covenants and conditions hereof to be performed, kept or observed by the Contractor shall be or be construed to be a waiver by the Port Authority of any other subsequent default in the performance of any of the said terms, covenants and conditions.

f) In addition to all other rights of revocation or termination hereunder and notwithstanding any other provision of this Contract the Port Authority may terminate this Contract and the rights of the Contractor hereunder without cause at any time upon five (5) days written notice to the Contractor and in such event this Contract shall cease and expire on the date set forth in the notice of termination as fully and completely as though such dates were the original expiration date hereof and if such effective date of termination is other than the last day of the month, the amount of the compensation due to the Contractor from the Port Authority shall be prorated when applicable on a daily basis. Such cancellation shall be without prejudice to the rights and obligations of the parties arising out of portions already performed but no allowance shall be made for anticipated profits.

g) Any right of termination contained in this paragraph, shall be in addition to and not in lieu of any and all rights and remedies that the Port Authority shall have at law or in equity consequent upon the Contractor's breach of this Contract and shall be without prejudice to any and all such other rights and remedies. It is hereby specifically agreed and understood that the exercise by the Port Authority of any right of termination set forth in this paragraph shall not be or be deemed to be an exercise by the Port Authority of an election of remedies so as to preclude the Port Authority from any right to money damages it may have for the period prior to the effective date of termination to the original expiration date of the Contract, and this provision shall be deemed to survive the termination of this Contract as aforesaid.

h) If (1) the Contractor fails to perform any of its obligations under this Contract or any other agreement between the Port Authority and the Contractor (including its obligation to the Port Authority to pay any claim lawfully made against it by any supplier, subcontractor or worker or other person which arises out of or in connection with the performance of this Contract or any other agreement with the Port Authority) or (2) any claim (just or unjust) which arises out of or in connection with this Contract or any other agreement between the Port Authority and the Contractor is made against the Port Authority or (3) any subcontractor under this Contract or any other agreement between the Port Authority and the Contractor fails to pay any claims lawfully made against it by any supplier, subcontractor, worker or other third person which arises out of or in connection with this Contract or any other agreement between the Port Authority and

the Contractor or if in the opinion of the Port Authority any of the aforesaid contingencies is likely to arise, then the Port Authority shall have the right, in its discretion, to withhold out of any payment (final or otherwise) such sums as the Port Authority may deem ample to protect it against delay or loss or to assure the payment of just claims of third persons, and to apply such sums in such manner as the Port Authority may deem proper to secure such protection or satisfy such claims. All sums so applied shall be deducted from the Contractor's compensation. Omission by the Port Authority to withhold out of any payment, final or otherwise, a sum for any of the above contingencies, even though such contingency has occurred at the time of such payment, shall not be deemed to indicate that the Port Authority does not intend to exercise its right with respect to such contingency. Neither the above provisions for rights of the Port Authority to withhold and apply monies nor any exercise or attempted exercise of, or omission to exercise, such rights by the Port Authority shall create any obligation of any kind to such supplier, subcontractors, worker or other third persons. If, however, the payment of any amount due the Contractor shall be improperly delayed, the Port Authority shall pay the Contractor interest thereon at the rate of 6% per annum for the period of the delay, it being agreed that such interest shall be in lieu of and in liquidation of any damages to the Contractor because of such delay.

i) If the Port Authority has paid any sum or has incurred any obligation or expense which the Contractor has agreed to pay or reimburse the Port Authority, or if the Port Authority is required or elects to pay any sum or sums or incurs any obligations or expense by reason of the failure, neglect or refusal of the Contractor to perform or fulfill any one or more of the conditions, covenants, or agreements contained in this Contract, or as a result of an act of omission of the Contractor contrary to the said conditions, covenants and agreements, the Contractor shall pay to the Port Authority the sum or sums so paid or expense so incurred, including all interests, costs and damages, promptly upon the receipt of the Port Authority's statement therefore. The Port Authority may, however, in its discretion, elect to deduct said sum or sums from any payment payable by it to the Contractor.

j) If the Port Authority pays any installment to the Contractor without reducing said installment as provided in this Contract, it may reduce any succeeding installment by the proper amount, or it may bill the Contractor for the amount by which the installment paid should have been reduced and the Contractor shall pay to the Port Authority any such amount promptly upon receipt of the Port Authority's statement therefore.

k) The Port Authority shall also have the rights set forth above in the event the Contractor shall become insolvent or bankrupt or if his affairs are placed in the hands of a receiver, trustee or assignee for the benefit of creditors.

12) CONTRACTOR PERSONNEL STANDARDS OF PERFORMANCE

The Contractor shall furnish sufficiently trained management, supervisory, technical and operating personnel to perform the services required of the Contractor under this Contract. If, in the opinion of the Director, any of the Contractor's personnel are not satisfactory in the performance of services to be furnished hereunder, the Contractor shall remove such personnel and replace them with personnel satisfactory to the Director.

At the time the Contractor is carrying out its operations there may be other persons working physically in the vicinity or in the same logical or technical infrastructure. The Contractor shall so conduct its operations as to work in harmony and not endanger, interfere with or delay the operations of others, all to the best interests of The Authority and others and as may be directed by the Director.

13) DESIGNATED SECURE AREAS

Services under the Contract may be required in designated secure areas, as the same may be designated by the Manager from time to time ("Secure Areas"). The Port Authority shall require the observance of certain security procedures with respect to Secure Areas, which may include the escort to, at, and/or from said high security areas by security personnel designated by the Contractor or any subcontractor's personnel required to work therein. All personnel that require access to designated secure areas who are not under positive escort by an authorized individual will be required to undergo background screening and personal identity verification.

Forty-eight (48) hours prior to the proposed performance of any work in a Secure Area, the Contractor shall notify the Manager. The Contractor shall conform to the procedures as may be established by the Manager from time to time and at any time for access to Secure Areas and the escorting of personnel hereunder. Prior to the start of work, the Contractor shall request a description from the Manager of the Secure Areas which will be in effect on the commencement date. The description of Secure Areas may be changed from time to time and at any time by the Manager during the term of the Contract.

14) NOTIFICATION OF SECURITY REQUIREMENTS

The Authority has the responsibility of ensuring safe, reliable and secure transportation facilities, systems, and projects to maintain the well-being and economic competitiveness of the region. Therefore, the Authority reserves the right to deny access to certain documents, sensitive security construction sites and facilities (including rental spaces) to any person that declines to abide by Port Authority security procedures and protocols, any person with a criminal record with respect to certain crimes or who may otherwise poses a threat to the construction site or facility security. The Authority reserves the right to impose multiple layers of security requirements on the Contractor, its staff and subcontractors and their staffs depending upon the level of security required, or may make any amendments with respect to such requirements as determined by the Authority.

These security requirements may include but are not limited to the following:

a) Contractor/ Subcontractor identity checks and background screening

The Port Authority's designated background screening provider may require inspection of not less than two forms of valid/current government issued identification (at least one having an official photograph) to verify staff's name and residence; screening federal, state, and/or local criminal justice agency information databases and files; screening of any terrorist identification files; access identification to include some form of biometric security methodology such as fingerprint, facial or iris scanning, or the like.

The Contractor may be required to have its staff, and any subcontractor's staff, materialmen, visitors or others over whom the Contractor/subcontractor has control, authorize the Authority or its designee to perform background checks, and a personal identity verification check. Such authorization shall be in a form acceptable to the Authority. The Contractor and subcontractors may also be required to use an organization designated by the Authority to perform the background checks.

As of January 29, 2007, the Secure Worker Access Consortium (S.W.A.C.) is the only Port Authority approved provider to be used to conduct background screening and personal identity verification, except as otherwise required by federal law and/or regulation (such as the Transportation Worker Identification Credential for personnel performing in secure areas at Maritime facilities). Information about S.W.A.C., instructions, corporate enrollment, online applications, and location of processing centers can be found at http://www.secureworker.com, or S.W.A.C. may be contacted directly at (877) 522-7922 for more information and the latest pricing. The cost for said background checks for staff that pass and are granted a credential shall be reimbursable to the Contractor (and its subcontractors) as an out-of-pocket expense as provided herein. Staff that are rejected for a credential for any reason are not reimbursable.

b) Issuance of Photo Identification Credential

No person will be permitted on or about the Authority construction site or facility (including rental spaces) without a facility-specific photo identification credential approved by the Authority. If the authority requires facility-specific identification credential for the Contractor's and the subcontractor's staff, the Authority will supply such identification at no cost to the Contractor or its subcontractors. Such facility-specific identification credential shall remain the property of the Authority and shall be returned to the Authority at the completion or upon request prior to completion of the individual's assignment at the specific facility. It is the responsibility of the appropriate Contractor or subcontractor to immediately report to the Authority the loss of any staff member's individual facility-specific identification credential. The Contractor or subcontractor shall be billed for the cost of the replacement identification credential. Contractor's and subcontractor's staff shall display Identification badges in a

conspicuous and clearly visible manner, when entering, working or leaving an Authority construction site or facility.

Employees may be required to produce not less than two forms of valid/current government issued identification having an official photograph and an original, unlaminated social security card for identify and SSN verification. Where applicable, for sensitive security construction sites or facilities, successful completion of the application, screening and identify verification for all employees of the Contractor and subcontractors shall be completed prior to being provided a S.W.A.C. ID Photo Identification credential.

c) Access control, inspection, and monitoring by security guards

The Authority may provide for Authority construction site or facility (including rental spaces) access control, inspection and monitoring by Port Authority Police or Authority retained contractor security guards. However, this provision shall not relieve the Contractor of its responsibility to secure its equipment and work and that of its subconsultant/subcontractors and service suppliers at the Authority construction site or facility (including rental spaces). In addition, the Contractor, subcontractor or service provider is not permitted to take photographs, digital images, electronic copying and/or electronic transmission or video recordings or make sketches on any other medium at the Authority construction sites or facilities (including rental spaces), except when necessary to perform the Work under this Contract, without prior written permission from the Authority. Upon request, any photograph, digital images, video recording or sketches made of the Authority construction site or facility shall be submitted to the Authority to determine compliance with this paragraph, which submission shall be conclusive and binding on the submitting entity.

d) Compliance with the Port Authority Information Security Handbook

The Contract may require access to Port Authority information considered Protected Information ("PI") as defined in the Port Authority Information Security Handbook ("Handbook"), dated October, 2008, corrected as of November 14, 2013, and as may be further amended. The Handbook and its requirements are hereby incorporated into this agreement and will govern the possession, distribution and use of PI if at any point during the lifecycle of the project or solicitation it becomes necessary for the Contractor to have access to PI. Protecting sensitive information requires the application of uniform safeguarding measures to prevent unauthorized disclosure and to control any authorized disclosure of this information within the Port Authority or when released by the Port Authority to outside entities. The following is an outline of some of the procedures, obligations and directives contained in the Handbook:

i) Require that the Contractor and subcontractors, when appropriate, sign Non-Disclosure Agreements (NDAs), or an Acknowledgment of an existing NDA, provided

by the Authority as a condition of being granted access to Confidential Information categorized and protected as per the Handbook;

ii) Require that individuals needing access to PI be required to undergo a background check, pursuant to the process and requirements noted in § 3.2 of the Information Security Handbook.

iii) Require Contractors and commercial enterprises to attend training to ensure security awareness regarding Port Authority information;

iv) Specific guidelines and requirements for the handling of PI to ensure that the storage and protection of PI;

v) Restrictions on the transfer, shipping, and mailing of PI;

vi) Prohibitions on the publication, posting, modifying, copying, reproducing, republishing, uploading, transmitting, or distributing PI on websites or web pages. This may also include restricting persons, who either have not passed a pre-screening background check, or who have not been granted access to PI, from viewing such information;

vii) Require that PI be destroyed using certain methods, measures or technology pursuant to the requirements set forth in the Handbook;

viii) Require the Contractor to mandate that each of its subcontractors maintain the same levels of security required of the Contractor under any Port Authority awarded contract.

ix) Prohibit the publication, exchange or dissemination of PI developed from the project or contained in reports, except between Contractors and subcontractors, without prior approval of the Port Authority;

x) Require that PI only be reproduced or copied pursuant to the requirements set forth in the Handbook.

e) <u>Audits for Compliance with Security Requirements</u>

The Port Authority may conduct random or scheduled examinations of business practices under this section entitled “NOTIFICATION OF SECURITY REQUIREMENTS” and the Handbook in order to assess the extent of compliance with security requirements, Confidential Information procedures, protocols and practices, which may include, but not be limited to, verification of background check status, confirmation of completion of specified training, and/or a site visit to view material storage locations and protocols.

The Authority may impose, increase, and/or upgrade security requirements for the Contractor, subcontractors and their staffs during the term of this Contract to address changing security conditions and/or new governmental regulations.

15) INSURANCE PROCURRED BY THE CONTRACTOR

The Contractor shall take out, maintain, and pay the premiums on Commercial General Liability Insurance, including but not limited to premises-operations, products-completed operations, and independent contractors coverage, with contractual liability language

covering the obligations assumed by the Contractor under this Contract and, if vehicles are to be used to carry out the performance of this Contract, then the Contractor shall also take out, maintain, and pay the premiums on Automobile Liability Insurance covering owned, non-owned, and hired autos in the following minimum limits:

a) **Commercial General Liability Insurance - $ 2 million** combined single limit per occurrence for bodily injury and property damage liability.
b) **Automobile Liability Insurance - $ 2 million** combined single limit per accident for bodily injury and property damage liability.

In addition, the liability policy (ies) shall name **The Port Authority of NY and NJ, its related entities, theirs commissioners, directors, officers, partners, employees and agents, The City of New York, AFCO AvPorts Management LLC and NY State Department of Transportation** as additional insured, including but not limited to premise-operations, products-completed operations on the Commercial General Liability Policy. Moreover, the Commercial General Liability Policy shall not contain any provisions for exclusions from liability other than provisions for exclusion from liability forming part of the most up to date ISO form or its equivalent unendorsed Commercial General Liability Policy. The liability policy (ies) and certificate of insurance shall contain cross-liability language providing severability of interests so that coverage will respond as if separate policies were in force for each insured. These insurance requirements shall be in effect for the duration of the contract to include any warrantee/guarantee period.

The certificate of insurance and liability policy (ies) must contain the following endorsement for the above liability coverages:

"The insurer(s) shall not, without obtaining the express advance written permission from the General Counsel of the Port Authority, raise any defense involving in any way the jurisdiction of the Tribunal over the person of the Port Authority, the immunity of the Port Authority, its Commissioners, officers, agents or employees, the governmental nature of the Port Authority, or the provisions of any statutes respecting suits against the Port Authority."

The Contractor shall also take out, maintain, and pay premiums on Workers' Compensation Insurance in accordance with the requirements of law in the state(s) where work will take place, and Employer's Liability Insurance with limits of not less than $1 million each accident.

Each policy above shall contain a provision that the policy may not be canceled, terminated, or modified without thirty (30) days' prior written notice to the Port Authority of NY and NJ, Att: Facility Contract Administrator, at the location where the work will take place and to the General Manager, Risk Financing.

The Port Authority may at any time during the term of this agreement change or modify the limits and coverages of insurance. Should the modification or change results in an additional premium, The General Manager, Risk Financing for the Port Authority may consider such cost as an out-of-pocket expense.

Within five (5) days after the award of this agreement or contract and prior to the start of work, the Contractor must submit an original certificate of insurance, to the Port Authority of NY and NJ, Facility Contract Administrator, at the location where the work will take place. This certificate of insurance MUST show evidence of the above insurance policy (ies), stating the agreement/contract number prior to the start of work. The General Manager, Risk Financing must approve the certificate(s) of insurance before any work can begin. Upon request by the Port Authority, the Contractor shall furnish to the General Manager, Risk Financing, a certified copy of each policy, including the premiums.

If at any time the above liability insurance should be canceled, terminated, or modified so that the insurance is not in effect as above required, then, if the Manager shall so direct, the Contractor shall suspend performance of the contract at the premises. If the contract is so suspended, no extension of time shall be due on account thereof. If the contract is not suspended (whether or not because of omission of the Manager to order suspension), then the Authority may, at its option, obtain insurance affording coverage equal to the above required, the cost of such insurance to be payable by the Contractor to the Port Authority.

Renewal certificates of insurance or policies shall be delivered to the Facility Contractor Administrator, Port Authority at least fifteen (15) days prior to the expiration date of each expiring policy. The General Manager, Risk Financing must approve the renewal certificate(s) of insurance before work can resume on the facility. If at any time any of the certificates or policies shall become unsatisfactory to the Port Authority, the Contractor shall promptly obtain a new and satisfactory certificate and policy.

The requirements for insurance procured by the Contractor shall not in any way be construed as a limitation on the nature or extent of the contractual obligations assumed by the Contractor under this contract. The insurance requirements are not a representation by the Authority as to the adequacy of the insurance to protect the Contractor against the obligations imposed on them by law or by this or any other Contract.

16) CERTAIN CONTRACTOR'S WARRANTIES

The Contractor represents and warrants:

a) That it is financially responsible and experienced in, and competent to perform this Contract; that no representation, promise or statement, oral or in writing, has induced it to submit its Proposal, saving only those contained in the papers expressly made part of this Contract; that the facts stated or shown in any papers submitted or referred to in connection with his Proposal are true; and, if the Contractor be a corporation, that it is authorized to perform this Contract;

b) That it has carefully examined and analyzed the provisions and requirements of this Contract, that from its own investigations it has satisfied itself as to the nature of all things needed for the performance of this Contract, the general and local conditions and all other matters which in any way affect this Contract or its performance, and that the time available to it for such examination, analysis, inspection and investigations was adequate;
c) That the Contract is feasible of performance in accordance with all its provisions and requirements and that it can and will perform it in strict accordance with such provisions and requirements;
d) That no Commissioner, officer, agent or employee of the Authority is personally interested directly or indirectly in this Contract or the compensation to be paid hereunder;
e) That, except only for those representations, statements or promises expressly contained in this Contract, no representation, statement or promise, oral or in writing, of any kind whatsoever by the Authority, its Commissioners, officers, agents, employees or consultants has induced the Contractor to enter into this Contract or has been relied upon by the Contractor, including any with reference to: (1) the meaning, correctness, suitability or completeness of any provisions or requirements of this Contract; (2) the nature, existence or location of materials, structures, obstructions, utilities or conditions, which may be encountered at the installation sites; (3) the nature, quantity, quality or size of the materials, equipment, labor and other facilities needed for the performance of this Contract; (4) the general or local conditions which may in any way affect this Contract or its performance; (5) the price of the Contract; or (6) any other matters, whether similar to or different from those referred to in (1) through (5) immediately above, affecting or having any connection with this Contract, the bidding thereon, any discussions thereof, the performance thereof or those employed therein or connected or concerned therewith.
f) That, notwithstanding any requirements of this Contract, any inspection or approval of the Contractor's services by the Authority, or the existence of any patent or trade name, the Contractor nevertheless warrants and represents that the services and any intellectual property supplied to the Authority hereunder shall be of the best quality and shall be fully fit for the purpose for which they are to be used. The Contractor unconditionally guarantees against defects or failures of any kind, including defects or failures in design, workmanship and materials, excepting solely defects or failures which the Contractor demonstrates to the satisfaction of the Authority have arisen solely from accident, abuse or fault of the Authority occurring after issuance of Final Payment hereunder and not due to fault on the Contractor's part. In the event of defects or failures in said services, or any part thereof, then upon receipt of notice thereof from the Authority, the Contractor shall correct such defects or failures as may be necessary or desirable, in the sole opinion of the Authority, to comply with the above guaranty.

Moreover, the Contractor accepts the conditions at the sites of work as they may eventually be found to exist and warrants and represents that it can and will perform the Contract under such conditions and that all materials, equipment, labor and other facilities required

because of any unforeseen conditions (physical or otherwise) shall be wholly at its own cost and expense, anything in this Contract to the contrary notwithstanding.

Nothing in the Scope of Work or any other part of the Contract is intended as or shall constitute a representation by the Authority as to the feasibility of performance of this Contract or any part thereof. Moreover, the Authority does not warrant or represent either by issuance of the Scope of Work or by any provision of this Contract as to time for performance or completion or otherwise that the Contract may be performed or completed by the times required herein or by any other times.

The Contractor further represents and warrants that it was given ample opportunity and time and by means of this paragraph was requested by the Authority to review thoroughly all documents forming this Contract prior to execution of this Contract in order that it might request inclusion in this Contract of any statement, representation, promise or provision which it desired or on which it wished to place reliance; that it did so review said documents; that either every such statement, representation, promise or provision has been included in this Contract or else, if omitted, that it expressly relinquishes the benefit of any such omitted statement, representation, promise or provision and is willing to perform this Contract without claiming reliance thereon or making any other claim on account of such omission.

The Contractor further recognizes that the provisions of this clause (though not only such provisions) are essential to the Authority's consent to enter into this Contract and that without such provisions; the Authority would not have entered into this Contract.

17) ASSIGNMENTS AND SUBCONTRACTS

Any assignment or other transfer by the Contractor of this Contract or any part hereof or of any of his rights hereunder or of any monies due or to become due hereunder and any delegation of any of his duties hereunder without the express written consent of the Director shall be void and of no effect as to the Authority, provided, however, that the Contractor may subcontract portions of the Work to such persons as the Director, may, from time to time, expressly approve in writing. For each individual, partnership or corporation proposed by the Contractor as a subcontractor, the Contractor shall submit to the Authority a certification or, if a certification cannot be made, a statement by such person, partnership or corporation to the same effect as the certification or statement required from the Contractor pursuant to the clauses of the Contractor's Integrity Provisions Section entitled "Certification of No Investigation Indictment, Conviction, Debarment Suspension, Disqualification and Disclosure of Other Information" and "Non-Collusive Bidding and Code of Ethics Certification; Certification of No Solicitation Based on Commission, Percentage, Brokerage Contingent or Other Fee". All further subcontracting by any subcontractor shall also be subject to such approval of the Director.

No consent to any assignment or other transfer, and no approval of any subcontractor, shall under any circumstances operate to relieve the Contractor of any of his obligations; no subcontract, no approval of any subcontractor and no act or omission of the Authority or the Director shall create any rights in favor of such subcontractor and against the Authority; and as between the Authority and the Contractor, all assignees, subcontractors, and other transferees shall for all purposes be deemed to be agents of the Contractor. Moreover, all subcontractors and all approvals of subcontractors, regardless of their form, shall be deemed to be conditioned upon performance by the subcontractor in accordance with this Contract; and if any subcontractor shall fail to perform the Contract to the satisfaction of the Director, the Director shall have the absolute right to rescind his approval forthwith and to require the performance of the Contract by the Contractor personally or through other approved subcontractors.

18) RIGHTS AND REMEDIES OF THE AUTHORITY

The Authority shall have the following rights in the event the Director shall deem the Contractor guilty of a breach of any term whatsoever of this contract:

a) The right to take over and complete the Work or any part thereof as agent for and at the expense of the Contractor, either directly or through other Contractors;
b) The right to cancel this Contract as to any or all of the Work yet to be performed;
c) The right to specific performance, an injunction or any other appropriate equitable remedy;
d) The right to money damages.

For the purpose of this Contract, breach shall include but not be limited to the following, whether or not the time has yet arrived for performance of an obligation under this Contract: a statement by the Contractor to any representative of The Authority indicating that he cannot or will not perform any one or more of his obligations under this Contract; any act or omission of the Contractor or any other occurrence which makes it improbable at the time that he will be able to perform any one or more of his obligations under this Contract; any suspension of or failure to proceed with any part of the Work by the Contractor which makes it improbable at the time that he will be able to perform any one or more of his obligations under this Contract; any false certification at any time by the Contractor as to any material item certified pursuant to the clauses hereof entitled "Certification of No Investigation (Criminal or Civil Anti-Trust), Indictment, Conviction, Debarment, Suspension, Disqualification and Disclosure of Other Required Information" and "Non-Collusive Bidding and Code of Ethics Certification; Certification of No Solicitation Based on Commission, Percentage, Brokerage, Contingent or Other Fee", or the willful or fraudulent submission of any signed statement pursuant to such clauses which is false in any material respect; or the Contractor's incomplete or inaccurate representation of its status with respect to the circumstances provided for in such clauses.

The enumeration in this numbered clause or elsewhere in this Contract of specific rights and remedies of The Authority shall not be deemed to limit any other rights or remedies which The Authority would have in the absence of such enumeration; and no exercise by The Authority of any right or remedy shall operate as a waiver of any other of its rights or remedies not inconsistent therewith or to stop it from exercising such other rights or remedies.

Neither the acceptance of the work or any part thereof, nor any payment therefor, nor any order or certificate issued under this Agreement or otherwise issued by the Authority, or any officer, agent or employee of the Authority, nor any permission or direction to continue with the performance or work, nor any performance by the authority of any of the Contractor's duties or obligations, nor any aid provided to the Contractor by the Authority in his performance of such duties or obligations, nor any other thing done or omitted to be done by the Authority, its Commissioners, officers, agents or employees shall be deemed to be a waiver of any provision of this agreement or of any rights or remedies to which the Authority may be entitled because of any breach hereof, excepting only a resolution of its Commissioners, providing expressly for such waiver. No cancellation, rescission or annulment hereof, in whole or as to any part of the work, because of any breach hereof, shall be deemed a waiver of any money damages to which the Authority may be entitled because of such breach. Moreover, no waiver by the Authority of any breach of this Agreement shall be deemed to be a waiver of any other or any subsequent breach.

19) RIGHTS AND REMEDIES OF THE CONTRACTOR

Inasmuch as the Contractor can be adequately compensated by money damages for any breach of this Contract which may be committed by the Authority, the Contractor expressly agrees that no default, act or omission of the Authority shall constitute a material breach of this Contract, entitling him to cancel or rescind it or (unless the Director shall so direct) to suspend or abandon performance.

20) TAX EXEMPTIONS

Purchases of services and tangible personal property by the Port Authority are exempt from New York and New Jersey state and local sales and compensating use taxes. (Sales Taxes). Therefore, the Port Authority's purchase of the Contractor's services under this Contract is exempt from Sales Taxes. Accordingly, the Contractor must not include Sales Taxes in the price charged to the Port Authority for the contractor's services under this Contract.

21) TITLE TO EQUIPMENT

Title to all equipment to be furnished hereunder by the Contractor shall be transferred to the Authority upon its delivery to the installation site.

The Contractor shall furnish such bills of sale and affidavits of title as the Authority shall reasonably request.

22) NOTICE REQUIREMENTS

No claim against the Authority shall be made or asserted in any action or proceeding at law or in equity, and the Contractor shall not be entitled to allowance of such claim, unless the Contractor shall have complied with all requirements relating to the giving of written notice and of information with respect to such claim as provided in this clause. The failure of the Contractor to give such written notice and information as to any claim shall be conclusively deemed to be a waiver by the Contractor of such claim, such written notice and information being conditions precedent to such claim. As used herein "claim" shall include any claim arising out of this agreement (including claims in the nature of breach of contract or fraud or misrepresentation before or subsequent to execution of this Agreement and claims of a type which are barred by the provisions of this agreement) for damages, payment or compensation of any nature or for performance of any part of this Agreement.

The requirements as to the giving of written notice and information with respect to claims shall be as follows:

a) In the case of any claims for which requirements are set forth elsewhere in this Agreement as to notice and information, such requirements shall apply.
b) In the case of all other types of claims, notice shall have been given to the Director, as soon as practicable, and in any case within forty eight (48) hours after occurrence of the act, omission, or other circumstances upon which the claim is or will be based, stating as fully as practicable at the time all information relating thereto. Such information shall be supplemented with any further information as soon as practicable after it becomes or should become known to the Contractor, including daily records showing all costs which the Contractor may be incurring or all other circumstances which will affect any claim to be made which records shall be submitted to the Authority.

The above requirements for notices and information are for the purpose of enabling the Authority to avoid waste of public funds by affording it promptly the opportunity to cancel or revise any order, change its plans, mitigate or remedy the effects of circumstances giving rise to a claim or take such other action as may seem desirable and to verify any claimed expense or circumstance as they occur and the requirements herein for such notice and information are essential to this Agreement and are in addition to any notice required by statue with respect to suits against the Authority.

The above referred to notices and information are required whether or not the Authority is aware of the existence of any circumstances which might constitute a basis for a claim and whether or not the Authority has indicated it will consider a claim.

No, act, omission or statement of any kind shall be regarded as a waiver of any of the provisions of this clause or may be relied upon as such waiver except only either a written statement signed by the Executive Director of the Authority or a resolution of the

Commissioners of the Authority expressly stating that a waiver is intended as to any particular provision of this clause, and more particularly, no discussion, negotiation, consideration, correspondence or requests for information with respect to a claim by any Commissioner, officer, employees or agent of the Authority shall be construed as a waiver of any provision of this clause or as authority or apparent authority to effect such a waiver.

Since merely oral notice or information may cause disputes as to the existence or substance thereof, and since notice, even if written, to other than the Authority representative above designated to receive it may not be sufficient to come to the attention of the representative of the Authority with the knowledge and responsibility of dealing with the situation, only notice and information complying with the express provisions of this clause shall be deemed to fulfill the Contractor's obligation under this Agreement.

23) SERVICE OF NOTICES ON THE CONTRACTOR

Whenever provision is made in this Contract for the giving of any notice to the Contractor, its deposit in any post office box, enclosed in a postpaid wrapper addressed to the Contractor at his/her office, or its delivery to his/her office, shall be sufficient service thereof as of the date of such deposit or delivery, except to the extent, if any, otherwise provided in the clause entitled "Submission to Jurisdiction". Until further notice to the Authority the Contractor's office will be that stated in his/her Proposal. Notices may also be served personally upon the Contractor; or if a corporation, upon any officer, director or managing or general agent; or if a partnership upon any partner.

24) NO THIRD PARTY RIGHTS

Nothing contained in this Agreement is intended for the benefit of third persons, except to the extent that the Agreement specifically provides otherwise by use of the words "benefit" or "direct right of action".

25) INDEMNIFICATION AND RISKS ASSUMED BY THE CONTRACTOR

To the extent permitted by law, the Contractor shall indemnify and hold harmless the Port Authority, its Commissioners, officers, representatives and employees from and against all claims and demands, just or unjust, of third persons (including Contractor's employees, employees, officers, and agents of the Port Authority) arising out of or in any way connected or alleged to arise out of or alleged to be in any way connected with the Contract and all other services and activities of the Contractor under this Contract and for all expenses incurred by it and by them in the defense, settlement or satisfaction thereof, including without limitation thereto, claims and demands for death, for personal injury or for property damage, direct or consequential, whether they arise from the acts or omissions of the Contractor, the Port Authority, third persons(including Contractor's employees, employees, officers, and agents of the Port Authority), or from the acts of God or the public

enemy, or otherwise, including claims and demands of any local jurisdiction against the Port Authority in connection with this Contract.

The Contractor assumes the following risks, whether such risks arise from acts or omissions (negligent or not) of the Contractor, the Port Authority or third persons (including Contractor's employees, employees, officers, and agents of the Port Authority)or from any other cause, excepting only risks occasioned solely by affirmative willful acts of the Port Authority done subsequent to the opening of proposals on this Contract, and shall to the extent permitted by law indemnify the Port Authority for all loss or damage incurred in connection with such risks:

a) The risk of any and all loss or damage to Port Authority property, equipment (including but not limited to automotive and/or mobile equipment), materials and possessions, on or off the premises, the loss or damage of which shall arise out of the Contractor's operations hereunder. The Contractor shall if so directed by the Port Authority, repair, replace or rebuild to the satisfaction of the Port Authority, any and all parts of the premises or the Facility which may be damaged or destroyed by the acts or omissions of the Contractor, its officers, agents, or employees and if the Contractor shall fail so to repair, replace, or rebuild with due diligence the Port Authority may, at its option, perform any of the foregoing work and the Contractor shall pay to the Port Authority the cost thereof.
b) The risk of any and all loss or damage of the Contractor's property, equipment (including but not limited to automotive and/or mobile equipment) materials and possessions on the Facility.
c) The risk of claim, whether made against the Contractor or the Port Authority, for any and all loss or damages occurring to any property, equipment (including but not limited to automotive and/or mobile equipment), materials and possessions of the Contractor's agents, employees, materialmen and others performing work hereunder.
d) The risk of claims for injuries, damage or loss of any kind just or unjust of third persons arising or alleged to arise out of the performance of work hereunder, whether such claims are made against the Contractor or the Port Authority.

If so directed, the Contractor shall at its own expense defend any suit based upon any such claim or demand, even if such suit, claim or demand is groundless, false or fraudulent, and in handling such shall not, without obtaining express advance permission from the General Counsel of the Port Authority, raise any defense involving in any way the jurisdiction of the tribunal over the person of the Port Authority, the immunity of the Port Authority, its Commissioners, officers, agents or employees, the governmental nature of the Port Authority or the provision of any statutes respecting suits against the Port Authority.

Neither the requirements of the Port Authority under this Contract, nor of the Port Authority of the methods of performance hereunder nor the failure of the Port Authority to call attention to improper or inadequate methods or to require a change in the method of performance hereunder nor the failure of the Port Authority to direct the Contractor to take

any particular precaution or other action or to refrain from doing any particular thing shall relieve the Contractor of its liability for injuries to persons or damage to property or environmental impairment arising out of its operations.

26) APPROVAL OF METHODS

Neither the approval of the Port Authority of the methods of furnishing services hereunder nor the failure of the Port Authority to call attention to improper or inadequate methods or to require a change in the method of furnishing services hereunder, nor the failure of the Port Authority to direct the Contractor to take any particular precautions or to refrain from doing any particular thing shall relieve the Contractor of its liability for injuries to persons or damage to property or environmental impairment arising out of its operations.

27) PORT AUTHORITY STANDARDS AND GUIDELINES FOR PORT AUTHORITY TECHNOLOGY AND SUPPLEMENTAL GUIDELINES FOR THE PORT AUTHORITY TECHNOLOGY SERVICES DEPARTMENT

The Contractor and any subcontractors shall follow the Port Authority Technology Standard and Guidelines and the Supplemental Guidelines for the Port Authority Technology Services Department attached hereto and made a part hereof, and shall comply with any updates to or changes in best practices related to such Standards and Guidelines.

28) SUBMISSION TO JURISDICTION

The Contractor hereby irrevocably submits itself to the jurisdiction of the Courts of the State of New York and New Jersey, in regard to any controversy arising out of, connected with, or in any way concerning this Contract.

The Contractor agrees that the service of process on the Contractor in relation to such jurisdiction may be made, at the option of the Port Authority, either by registered or certified mail addressed to it at the address of the Contractor indicated on the signature sheet, or by actual personal delivery to the Contractor, if the Contractor is an individual, to any partner if the Contractor be a partnership or to any officer, director or managing or general agent if the Contractor be a corporation.

Such service shall be deemed to be sufficient when jurisdiction would not lie because of the lack of basis to serve process in the manner otherwise provided by law. In any case, however, process may be served as stated above whether or not it might otherwise have been served in a different manner.

29) APPLICABLE LAW

This Contract shall be construed in accordance with the laws of the State of New York. The Contractor hereby consents to the exercise by the courts of the States of New York and New

Jersey of jurisdiction in personam over it with respect to any matter arising out of or in connection with this Contract and waives any objection to such jurisdiction which it might otherwise have; and the Contractor agrees that mailing of process by registered mail addressed to it at the address of the Contractor set forth in the Proposal, shall have the same effect as personal service within the States of New York or New Jersey upon a domestic corporation of said State.

30) AUTHORITY OF THE DIRECTOR

Inasmuch as the public interest requires that the Project to which this Contract relates shall be performed in the manner which the Authority, acting through the Director, deems best, the Director shall have absolute authority to determine what is or is not necessary or proper for or incidental thereto and the Specifications shall be deemed merely the Director's present determination on this point. In the exercise of this authority, the Director shall have power to alter the Specifications, to require the performance of Work not required by them in their present form, even though of a totally different character from that not required, and to vary, increase and diminish the character, quantity and quality of, or to countermand any Work now or hereafter required. If at any time it shall be, from the viewpoint of the Authority, impracticable or undesirable in the judgment of the Director to proceed with or continue the performance of the Contract or any part thereof, whether or not for reasons beyond the control of the Authority, the Director shall have authority to suspend performance of any part or all of the Contract until such time as the Director may deem it practicable or desirable to proceed. Moreover, if at any time it shall be, from the viewpoint of the Authority impracticable or undesirable in the judgment of the Director to proceed with or continue the performance of the Contract or any part thereof for reasons within or beyond the control of the Authority, the Director shall have authority to cancel this Contract as to any or all portions not yet performed and as to any materials not yet installed even though delivered. Such cancellation shall be without prejudice to the rights and obligations of the parties arising out of portions already satisfactorily performed, but no allowance shall be made for anticipated profits. To resolve all disputes and to prevent litigation, the parties to this Contract authorize the Director to decide all questions of any nature whatsoever arising out of, under, or in connection with, or in any way related to or on account of, this Contract (including claims in the nature of breach of contract or fraud or misrepresentation before or subsequent to acceptance of the Contractor's Proposal and claims of a type which are barred by the provisions of this Contract) and such decision shall be conclusive, final and binding on the parties. The Director's decision may be based on such assistance as she may find desirable. The effect of the decision shall not be impaired or waived by any negotiation or settlement offers in connection with the question decided, whether or not she participated therein, or by any prior decision of her or others, which prior decisions shall be deemed subject to review, or by any termination or cancellation of this Contract.

All such questions shall be submitted in writing by the Contractor to the Director for a decision together with all evidence and other pertinent information in regard to such

questions, in order that a fair and impartial decision may be made. In any action against the Authority relating to any such question the Contractor must allege in the complaint and prove such submission, which shall be a condition precedent to any such action. No evidence or information shall be introduced or relied upon in such an action that has not been so presented to the Director.

In the performance of the Contract, the Contractor shall conform to all orders, directions and requirements of the Director and shall perform the Contract to her satisfaction at such times and places, by such methods and such manner and sequence as she may require, and the Contract shall at all stages be subject to her inspection. The Contractor shall employ no equipment, materials, methods or men to which she objects, and shall remove no materials, equipment or other facilities from the Authority site without permission. Upon request, she shall confirm in writing any oral order, direction, requirements or determination.

The enumeration herein or elsewhere of particular instances in which the opinion, judgment, discretion or determination of the Director shall control or in which the Contract shall be performed to her satisfaction or subject to her inspection, shall not imply that only the matters of a nature similar to those enumerated shall be so governed and performed, but without exception the entire Contract shall be so governed and performed.

This provision shall be construed in accordance with the laws of the State of New York excluding its conflict of law provisions.

31) APPROVALS BY THE DIRECTOR

The approval by the Director of any service required hereunder, shall be construed merely to mean that at that time the Director knows of no good reason for objecting thereto and no such approval shall release the Contractor from its full responsibility for the satisfactory performance of the services to be supplied. "Approved equal" shall mean approved by the Director.

32) CONTRACT REVIEW AND COMPLIANCE AUDITS

The Contractor, and any subcontractors, shall provide system access and reasonable assistance to the Authority's External and Internal Audit staff or its consultants in their performance of work under the contract, including producing specific requested information, extraction of data and reports. The Contractor, and any subcontractors, shall support requests related to audits of the agreement and administration tasks and functions covered by this Contract.

The Authority reserves the right to use and load security and system software to evaluate the level of security and vulnerabilities in all systems, which control, collect, dispense, contain, manage, administer, or monitor revenue "owned" by the Port Authority.

The Authority reserves the right to use as required and load security and system software to evaluate the level of security and vulnerabilities in any applicable environment covered under this Contract. If such right is exercised, then both parties shall work in good faith to ensure there is no access or potential access to third party proprietary data within the applicable environment or access to other systems not covered under this Contract.

33) AUTHORITY ACCESS TO RECORDS

The Authority shall have access during normal business hours to all records and documents of the Contractor relating to any service provided under this Agreement, amounts for which it has been compensated, or claims he should be compensated, by The Authority above those included in the lump sum compensation set forth elsewhere herein. All Contractor records shall be kept in the Port District. The Contractor shall obtain for The Authority similar access to similar records and documents of subcontractors. Such access shall be given or obtained both before and within a period of three (3) years after Final Payment to the Contractor, provided, however, that if within the aforesaid one year period The Authority has notified the Contractor in writing of a pending claim by The Authority under or in connection with this Contract to which any of the aforesaid records and documents of the Contractor or of his subcontractors relate either directly or indirectly, then the period of such right of access shall be extended to the expiration of six (6) years from the date of Final Payment with respect to the records and documents involved.

Upon request of the Port Authority, the Contractor shall furnish or provide access to the federal Form I-9 (Employment Eligibility Verification) for each individual performing work under this Contract. This includes citizens and noncitizens.

The Contractor shall provide, at no cost to the Authority, access for and reasonable assistance to such auditors from the Authority or the Authority's external auditors that may, from time to time, be designated to audit detail records which support Contractor charges to the Authority. The Authority shall have access to the detail records that support Contractor charges to the Authority for up to three (3) years following the termination of the Contract.

No provision in this Contract giving The Authority a right of access to records and documents is intended to impair or affect any right of access to records and documents that The Authority would have in the absence of such provision.

34) HARMONY

a) The Contractor shall not employ any persons or use any labor, or use or have any equipment, or permit any condition to exist which shall or may cause or be conducive to any labor complaints, troubles, disputes or controversies at the Facility which interfere or are likely to interfere with the operation of the Port Authority or with the operations

of lessees, licensees or other users of the Facility or with the operations of the Contractor under this Contract.

The Contractor shall immediately give notice to the Port Authority (to be followed by written notices and reports) of any and all impending or existing labor complaints, troubles, disputes or controversies and the progress thereof. The Contractor shall use its best efforts to resolve any such complaint, trouble, dispute or controversy. If any type of strike, boycott, picketing, work stoppage, slowdown or other labor activity is directed against the Contractor at the Facility or against any operations of the Contractor under this Contract, whether or not caused by the employees of the Contractor, and if any of the foregoing, in the opinion of the Port Authority, results or is likely to result in any curtailment or diminution of the services to be performed hereunder or to interfere with or affect the operations of the Port Authority , or to interfere with or affect the operations of lessees, licensees, or other users of the Facility or in the event of any other cessation or stoppage of operations by the Contractor hereunder for any reason whatsoever, the Port Authority shall have the right at any time during the continuance thereof to suspend the operations of the Contractor under this Contract, and during the period of the suspension the Contractor shall not perform its services hereunder and the Port Authority shall have the right during said period to itself or by any third person or persons selected by it to perform said services of the Contractor using the equipment which is used by the Contractor in its operations hereunder as the Port Authority deems necessary and without cost to the Port Authority. During such time of suspension, the Contractor shall not be entitled to any compensation. Any flat fees, including management fees, shall be prorated. Prior to the exercise of such right by the Port Authority, it shall give the Contractor notice thereof, which notice may be oral. No exercise by the Port Authority of the rights granted to it in the above subparagraph shall be or be deemed to be a waiver of any rights of termination or revocation contained in this Contract or a waiver of any rights or remedies which may be available to the Port Authority under this Contract or otherwise.

b) During the time that the Contractor is performing the Contract, other persons may be engaged in other operations on or about the worksite including Facility operations, pedestrian, bus and vehicular traffic and other Contractors performing at the worksite, all of which shall remain uninterrupted.

The Contractor shall so plan and conduct its operations as to work in harmony with others engaged at the site and not to delay, endanger or interfere with the operation of others (whether or not specifically mentioned above), all to the best interests of the Port Authority and the public as may be directed by the Port Authority.

35) CLAIMS OF THIRD PERSONS

The Contractor undertakes to pay all claims lawfully made against him by subcontractors, materialmen and workmen, and all claims lawfully made against him by other third persons

arising out of or in connection with or because of the performance of this Contract and to cause all subcontractors to pay all such claims lawfully made against them.

36) NON-DISCRIMINATION REQUIREMENTS

The Contractor shall take all necessary and reasonable steps to ensure non-discrimination in the performance and administration of all aspects of this Contract.

a) Contractor hereby agrees that no person on the ground of race, color, national origin, creed/religion, sex, age or handicap/disability shall be excluded from participation in, denied the benefits of, or be otherwise subjected to discrimination in the furnishing of goods or services or in the selection and retention of subcontractors and/or vendors under this Contract. Contractor shall also ascertain and comply with all applicable federal, state and local laws, ordinances, rules, regulations, and orders that pertain to equal employment opportunity, affirmative action, and non-discrimination in employment.

b) Contractor agrees that these "Non-Discrimination Requirements" are a binding part of this Contract. Without limiting the generality of any other term or provision of this Contract, in the event the Authority, or a state or federal agency finds that the Contractor or any of its subcontractors or vendors has not complied with these "Non-Discrimination Requirements", the Authority may cancel, terminate or suspend this Contract in accordance with Section 11 of these Terms and Conditions entitled "Default, Revocation, or Suspension of Contract."

c) Contractor agrees to cooperate fully with the Authority's investigation of allegations of discrimination. Cooperation includes, but is not limited to, allowing the Authority to question employees during the investigation of allegations of discrimination, and complying with directives that the Authority or the State or Federal government deem essential to ensure compliance with these "Non-Discrimination Requirements."

37) CONTRACTOR'S INTEGRITY PROVISIONS

a) Certification of No Investigation (criminal or civil anti-trust), Indictment, Conviction, Debarment, Suspension, Disqualification and Disclosure of Other Information

By bidding on this Contract, each Bidder and each person signing on behalf of any Bidder certifies, and in the case of a joint bid each party thereto certifies as to its own organization, that the Bidder and each parent and/or affiliate of the Bidder has not

i) Been Indicted Or Convicted In Any Jurisdiction;
ii) Been Suspended, Debarred, Found Not Responsible Or Otherwise Disqualified From Entering Into Any Contract With Any Governmental Agency Or Been Denied A

Government Contract For Failure To Meet Standards Related To The Integrity Of The Bidder;

iii) Had A Contract Terminated By Any Governmental Agency For Breach Of Contract Or For Any Cause Based In Whole Or In Part On An Indictment Or Conviction;

iv) Ever Used A Name, Trade Name Or Abbreviated Name, Or An Employer Identification Number Different From Those Inserted In The Bid;

v) Had Any Business Or Professional License Suspended Or Revoked Or, Within The Five Years Prior To Bid Opening, Had Any Sanction Imposed In Excess Of Fifty Thousand Dollars ($50,000) As A Result Of Any Judicial Or Administrative Proceeding With Respect To Any License Held Or With Respect To Any Violation Of A Federal, State Or Local Environmental Law, Rule Or Regulation;

vi) Had Any Sanction Imposed As A Result Of A Judicial Or Administrative Proceeding Related To Fraud, Extortion, Bribery, Bid Rigging, Embezzlement, Misrepresentation Or Anti-Trust Regardless Of The Dollar Amount Of The Sanctions Or The Date Of Their Imposition; And

vii) Been, And Is Not Currently, The Subject Of A Criminal Investigation By Any Federal, State Or Local Prosecuting Or Investigative Agency And/Or A Civil Anti-Trust Investigation By Any Federal, State Or Local Prosecuting Or Investigative Agency, Including An Inspector General Of A Governmental Agency Or Public Authority.

b) Non-Collusive Bidding, and Code of Ethics Certification, Certification of No Solicitation Based On Commission, Percentage, Brokerage, Contingent or Other Fees

By bidding on this Contract, each Bidder and each person signing on behalf of any Bidder certifies, and in the case of a joint bid, each party thereto certifies as to its own organization, that

i) the prices in its bid have been arrived at independently without collusion, consultation, communication or agreement for the purpose of restricting competition, as to any matter relating to such prices with any other bidder or with any competitor;

ii) the prices quoted in its bid have not been and will not be knowingly disclosed directly or indirectly by the Bidder prior to the official opening of such bid to any other bidder or to any competitor;

iii) no attempt has been made and none will be made by the Bidder to induce any other person, partnership or corporation to submit or not to submit a bid for the purpose of restricting competition;

iv) this organization has not made any offers or agreements or taken any other action with respect to any Authority employee or former employee or immediate family member of either which would constitute a breach of ethical standards under the Code of Ethics dated March 11, 2014, or as may be revised, (a copy of which is available upon request) nor does this organization have any knowledge of any act on the part of an Authority employee or former Authority employee relating either

directly or indirectly to this organization which constitutes a breach of the ethical standards set forth in said Code;

v) no person or selling agency other than a bona fide employee or bona fide established commercial or selling agency maintained by the Bidder for the purpose of securing business, has been employed or retained by the Bidder to solicit or secure this Contract on the understanding that a commission, percentage, brokerage, contingent, or other fee would be paid to such person or selling agency; and

vi) the Bidder has not offered, promised or given, demanded or accepted, any undue advantage, directly or indirectly, to or from a public official or employee, political candidate, party or party official, or any private sector employee (including a person who directs or works for a private sector enterprise in any capacity), in order to obtain, retain, or direct business or to secure any other improper advantage in connection with this Contract.

vii) no person or organization has been retained, employed or designated on behalf of the Bidder to impact any Port Authority determination with respect to (i) the solicitation, evaluation or award of this Contract, or (ii) the preparation of specifications or request for submissions in connection with this Contract.

The foregoing certifications in 38 (1) and 38 (2) above, shall be deemed to have been made by the Bidder as follows:

(1) if the Bidder is a corporation, such certification shall be deemed to have been made not only with respect to the Bidder itself, but also with respect to each parent, affiliate, director, and officer of the Bidder, as well as, to the best of the certifier's knowledge and belief, each stockholder of the Bidder with an ownership interest in excess of 10%;

(2) if the Bidder is a partnership, such certification shall be deemed to have been made not only with respect to the Bidder itself, but also with respect to each partner.

Moreover, the foregoing certifications, if made by a corporate Bidder, shall be deemed to have been authorized by the Board of Directors of the Bidder, and such authorization shall be deemed to include the signing and submission of the bid and the inclusion therein of such certification as the act and deed of the corporation.

In any case where the Bidder cannot make the foregoing certifications, the Bidder shall so state and shall furnish with the signed bid a signed statement which sets forth in detail the reasons therefor. If the Bidder is uncertain as to whether it can make the foregoing certifications, it shall so indicate in a signed statement furnished with its bid, setting forth in such statement the reasons for its uncertainty. With respect to the foregoing certification in paragraph “2g”, if the Bidder cannot make the certification, it shall provide, in writing, with the signed bid: (i) a list of the name(s), address(es), telephone number(s), and place(s) of principal employment of each such individual or

organization; and (ii) a statement as to whether such individual or organization has a "financial interest" in this Contract, as described in the Procurement Disclosure Policy of the Authority (a copy of which is available upon request to the Chief Procurement Officer of the Procurement Department of the Authority). Such disclosure is to be updated, as necessary, up to the time of award of this Contract. As a result of such disclosure, the Port Authority shall take appropriate action up to and including a finding of non-responsibility.

Failure to make the required disclosures shall lead to administrative actions up to and including a finding of non-responsiveness or non-responsibility.

Notwithstanding that the Bidder may be able to make the foregoing certifications at the time the bid is submitted, the Bidder shall immediately notify the Authority in writing during the period of irrevocability of bids and the term of the Contract, if Bidder is awarded the Contract, of any change of circumstances which might under this clause make it unable to make the foregoing certifications, might render any portion of the certifications previously made invalid, or require disclosure. The foregoing certifications or signed statement shall be deemed to have been made by the Bidder with full knowledge that they would become a part of the records of the Authority and that the Authority will rely on their truth and accuracy in awarding and continuing this Contract. In the event that the Authority should determine at any time prior or subsequent to the award of this Contract that the Bidder has falsely certified as to any material item in the foregoing certifications, has failed to immediately notify the Port Authority of any change in circumstances which might make it unable to make the foregoing certifications, might render any portion of the certifications previously made invalid, or require disclosure, or has willfully or fraudulently furnished a signed statement which is false in any material respect, or has not fully and accurately represented any circumstance with respect to any item in the foregoing certifications required to be disclosed, the Authority may determine that the Bidder is not a responsible Bidder with respect to its bid on the Contract or with respect to future bids on Authority contracts and may exercise such other remedies as are provided to it by the Contract with respect to these matters. In addition, Bidders are advised that knowingly providing a false certification or statement pursuant hereto may be the basis for prosecution for offering a false instrument for filing (see e.g. New York Penal Law, Section 175.30 et seq.). Bidders are also advised that the inability to make such certification will not in and of itself disqualify a Bidder, and that in each instance the Authority will evaluate the reasons therefor provided by the Bidder. Under certain circumstances the Bidder may be required as a condition of Contract award to enter into a Monitoring Agreement under which it will be required to take certain specified actions, including compensating an independent Monitor to be selected by the Port Authority, said Monitor to be charged with, among other things, auditing the actions of the Bidder to determine whether its business practices and relationships indicate a level of integrity sufficient to permit it to continue business with the Port Authority.

c) Bidder Eligibility for Award of Contracts - Determination by an Agency of the State of New York or New Jersey Concerning Eligibility to Receive Public Contracts

Bidders are advised that the Authority has adopted a policy to the effect that in awarding its contracts it will honor any determination by an agency of the State of New York or New Jersey that a Bidder is not eligible to bid on or be awarded public contracts because the Bidder has been determined to have engaged in illegal or dishonest conduct or to have violated prevailing rate of wage legislation.

The policy permits a Bidder whose ineligibility has been so determined by an agency of the State of New York or New Jersey to submit a bid on a Port Authority contract and then to establish that it is eligible to be awarded a contract on which it has bid because (i) the state agency determination relied upon does not apply to the Bidder, or (ii) the state agency determination relied upon was made without affording the Bidder the notice and hearing to which the Bidder was entitled by the requirements of due process of law, or (iii) the state agency determination was clearly erroneous or (iv) the state determination relied upon was not based on a finding of conduct demonstrating a lack of integrity or violation of a prevailing rate of wage law.

The full text of the resolution adopting the policy may be found in the Minutes of the Authority's Board of Commissioners meeting of September 9, 1993.

d) Contractor Responsibility, Suspension of Work and Termination

During the term of this Contract, the Contractor shall at all times during the Contract term remain responsible. The Contractor agrees, if requested by the Port Authority to present evidence of its continuing legal authority to do business in the States of New Jersey or New York, integrity, experience, ability, prior performance, and organizational and financial capacity.

The Port Authority, in its sole discretion, reserves the right to suspend any or all activities under this Contract, at any time, when it discovers information that calls into question the responsibility of the Contractor. In the event of such suspension, the Contractor will be given written notice outlining the particulars of such suspension. Upon issuance of such notice, the Contractor must comply with the terms of the suspension order. Contract activity may resume at such time as the Port Authority issues a written notice authorizing a resumption of performance under the Contract.

Upon written notice to the Contractor, and an opportunity to be heard with appropriate Port Authority officials or staff, the Contract may be terminated by Port Authority at the Contractor's expense where the Contractor is determined by the Port Authority to be non-responsible. In such event, the Port Authority or its designee may complete the contractual requirements in any manner he or she may deem advisable and pursue

available legal or equitable remedies for breach, including recovery of costs from Contractor associated with such termination.

e) No Gifts, Gratuities, Offers of Employment, Etc.
At all times, the Contractor shall not offer, give or agree to give anything of value either to a Port Authority employee, agent, job shopper, consultant, construction manager or other person or firm representing the Port Authority, or to a member of the immediate family (i.e., a spouse, child, parent, brother or sister) of any of the foregoing, in connection with the performance by such employee, agent, job shopper, consultant, construction manager or other person or firm representing the Port Authority of duties involving transactions with the Contractor on behalf of the Port Authority, whether or not such duties are related to this Contract or any other Port Authority contract or matter. Any such conduct shall be deemed a material breach of this Contract.

As used herein "anything of value" shall include but not be limited to any (a) favors, such as meals, entertainment, transportation (other than that contemplated by the Contract or any other Port Authority contract), etc. which might tend to obligate the Port Authority employee to the Contractor, and (b) gift, gratuity, money, goods, equipment, services, lodging, discounts not available to the general public, offers or promises of employment, loans or the cancellation thereof, preferential treatment or business opportunity. Such term shall not include compensation contemplated by this Contract or any other Port Authority contract. Where used herein, the term "Port Authority" shall be deemed to include all subsidiaries of the Port Authority.

The Contractor shall insure that no gratuities of any kind or nature whatsoever shall be solicited or accepted by it and by its personnel for any reason whatsoever from the passengers, tenants, customers or other persons using the Facility and shall so instruct its personnel.

In the event that the Contractor becomes aware of the occurrence of any conduct that is prohibited by this section entitled “No Gifts, Gratuities, Offers of Employment, Etc.”, it shall report such occurrence to the Port Authority’s Office of Inspector General within three (3) business days of obtaining such knowledge. (See “http://www.panynj.gov/inspector-general” for information about to report information to the Office of Inspector General). Failing to report such conduct shall be grounds for a finding of non-responsibility.

In addition, during the term of this Contract, the Contractor shall not make an offer of employment or use confidential information in a manner proscribed by the Code of Ethics and Financial Disclosure dated March 11, 2014, or as may be revised (a copy of which is available upon request to the Office of the Secretary of the Port Authority).

The Contractor shall include the provisions of this clause in each subcontract entered into under this Contract.

f) Conflict of Interest

During the term of this Contract, the Contractor shall not participate in any way in the preparation, negotiation or award of any contract (other than a contract for its own services to the Authority) to which it is contemplated the Port Authority may become a party, or participate in any way in the review or resolution of a claim in connection with such a contract if the Contractor has a substantial financial interest in the contractor or potential contractor of the Port Authority or if the Contractor has an arrangement for future employment or for any other business relationship with said contractor or potential contractor, nor shall the Contractor at any time take any other action which might be viewed as or give the appearance of conflict of interest on its part. If the possibility of such an arrangement for future employment or for another business arrangement has been or is the subject of a previous or current discussion, or if the Contractor has reason to believe such an arrangement may be the subject of future discussion, or if the Contractor has any financial interest, substantial or not, in a contractor or potential contractor of the Authority, and the Contractor's participation in the preparation, negotiation or award of any contract with such a contractor or the review or resolution of a claim in connection with such a contract is contemplated or if the Contractor has reason to believe that any other situation exists which might be viewed as or give the appearance of a conflict of interest, the Contractor shall immediately inform the Chief Procurement Officer in writing of such situation giving the full details thereof. Unless the Contractor receives the specific written approval of the Chief Procurement Officer, the Contractor shall not take the contemplated action which might be viewed as or give the appearance of a conflict of interest. The Chief Procurement Officer may require the Contractor to submit a mitigation plan addressing and mitigating any disclosed or undisclosed conflict, which is subject to the approval of the Chief Procurement Officer and shall become a requirement, as though fully set forth in this Contract. In the event the Chief Procurement Officer shall determine that the performance by the Contractor of a portion of its Services under this Agreement is precluded by the provisions of this numbered paragraph, or a portion of the Contractor's said Services is determined by the Chief Procurement Officer to be no longer appropriate because of such preclusion, then the Chief Procurement Officer shall have full authority on behalf of both parties to order that such portion of the Contractor's Services not be performed by the Contractor, reserving the right, however, to have the Services performed by others and any lump sum compensation payable hereunder which is applicable to the deleted work shall be equitably adjusted by the parties. The Contractor's execution of this document shall constitute a representation by the Contractor that at the time of such execution the Contractor knows of no circumstances, present or anticipated, which come within the provisions of this paragraph or which might otherwise be viewed as or give the appearance of a conflict of interest on the Contractor's part. The Contractor acknowledges that the Authority may preclude it from involvement in certain disposition/privatization initiatives or transactions that result from the findings of its evaluations hereunder or from

participation in any contract, which results, directly or indirectly, from the Services provided by the Contractor hereunder. The Port Authority's determination regarding any questions of conflict of interest shall be final.

g) Definitions

As used in this Section 38, the following terms shall mean:

Affiliate - Two or more firms are affiliates if a parent owns more than fifty percent of the voting stock of each of the firms, or a common shareholder or group of shareholders owns more than fifty percent of the voting stock of each of the firms, or if the firms have a common proprietor or general partner.

Agency or Governmental Agency - Any federal, state, city or other local agency, including departments, offices, public authorities and corporations, boards of education and higher education, public development corporations, local development corporations and others.

Investigation - Any inquiries made by any federal, state or local criminal prosecuting and/or law enforcement agency and any inquiries concerning civil anti-trust investigations made by any federal, state or local governmental agency. Except for inquiries concerning civil anti-trust investigations, the term does not include inquiries made by any civil government agency concerning compliance with any regulation, the nature of which does not carry criminal penalties, nor does it include any background investigations for employment, or Federal, State, and local inquiries into tax returns.

Officer - Any individual who serves as chief executive officer, chief financial officer, or chief operating officer of the Bidder by whatever titles known.

Parent - An individual, partnership, joint venture or corporation which owns more than 50% of the voting stock of the Bidder.

If the solicitation is a Request for Proposal:

Bid - shall mean Proposal;
Bidder - shall mean Proposer;
Bidding - shall mean submitting a Proposal

In a Contract resulting from the taking of bids:

Bid - shall mean bid;
Bidder - shall mean Bidder; except and until the Contract has been awarded, then it shall mean Contractor
Bidding - shall mean executing this Contract.

In a Contract resulting from the taking of Proposals:

Bid - shall mean Proposal;
Bidder - shall mean Proposer;
Bidding - shall mean executing this Contract.

38) CONFIDENTIAL INFORMATION/NON-PUBLICATION

a) As used herein, confidential information shall mean all information disclosed to the Contractor or the personnel provided by the Contractor hereunder which relates to the Authority's and/or PATH's past, present, and future research, development and business activities including, but not limited to, software and documentation licensed to the Authority or proprietary to the Authority and/or PATH and all associated software, source code procedures and documentation. Confidential information shall also mean any other tangible or intangible information or materials including but not limited to computer identification numbers, access codes, passwords, and reports obtained and/or used during the performance of the Contractor's Services under this Contract.

b) Confidential information shall also mean and include collectively, as per The Port Authority of New York & New Jersey Information Security Handbook (October 15, 2008, corrected as of November 14, 2013), Protected Information, Confidential Proprietary Information, Confidential Privileged Information and information that is labeled, marked or otherwise identified by or on behalf of the Authority so as to reasonably connote that such information is confidential, privileged, sensitive or proprietary in nature. Confidential Information shall also include all work product that contains or is derived from any of the foregoing, whether in whole or in part, regardless of whether prepared by the Authority or a third-party or when the Authority receives such information from others and agrees to treat such information as Confidential.

c) The Contractor shall hold all such confidential information in trust and confidence for the Authority, and agrees that the Contractor and the personnel provided by the Contractor hereunder shall not, during or after the termination or expiration of this Contract, disclose to any person, firm or corporation, nor use for its own business or benefit, any information obtained by it under or in connection with the supplying of services contemplated by this Contract. The Contractor and the personnel provided by the Contractor hereunder shall not violate in any manner any patent, copyright, trade secret or other proprietary right of the Authority or third persons in connection with their services hereunder, either before or-after termination or expiration of this Contract. The Contractor and the personnel provided by the Contractor hereunder shall not willfully or otherwise perform any dishonest or fraudulent acts, breach any security procedures, or damage or destroy any hardware, software or documentation, proprietary or otherwise, in connection with their services hereunder. The Contractor shall promptly and fully inform the Director/General Manager in writing of any patent, copyright, trade secret or other intellectual property rights or disputes, whether existing or potential, of which the Contractor has knowledge, relating to any idea, design,

method, material, equipment or other matter related to this Contract or coming to the Contractor's attention in connection with this Contract."

d) The Contractor shall not issue nor permit to be issued any press release, advertisement, or literature of any kind, which refers to the Port Authority or to the fact that goods have been, are being or will be provided to it and/or that services have been, are being or will be performed for it in connection with this Agreement, unless the vendor first obtains the written approval of the Port Authority. Such approval may be withheld if for any reason the Port Authority believes that the publication of such information would be harmful to the public interest or is in any way undesirable.

39) PROVISIONS OF LAW DEEMED INSERTED

Each and every provision of law and clause required by law to be inserted in this Contract shall be deemed to be inserted herein and the Contract shall be read and enforced as though it were included therein, and if through mistake or otherwise any such provision is not inserted, or is not correctly inserted, then upon the application of either party, the Contract shall forthwith be physically amended to make such insertion.

40) INVALID CLAUSES

If any provision of this Contract shall be such as to destroy its mutuality or to render it invalid or illegal, then if it shall not appear to have been so material that without it the Contract would not have been made by the parties, it shall not be deemed to form part thereof but the balance of the Contract shall remain in full force and effect.

41) NO ESTOPPEL OR WAIVER

The Authority shall not be precluded or estopped by any acceptance, certificate or payment, final or otherwise, issued or made under this Contract or otherwise issued or made by it, the Director or any officer, agent or employee of The Authority, from showing at any time the true amount and character of Work performed, or from showing that any such acceptance, certificate or payment is incorrect or was improperly issued or made; and The Authority shall not be precluded or estopped, notwithstanding any such acceptance, certificate or payment, from recovering from the Contractor any damages which it may sustain by reason of any failure on his part to comply strictly with this Contract, and any monies which may be paid to him or for his account in excess of those to which he is lawfully entitled.

42) NON-LIABILITY OF THE AUTHORITY REPRESENTATIVES

Neither the Commissioners of the Authority, nor any officer, agent, or employee thereof shall be charged personally by the Contractor with any liability or held liable under any term

or provision of this Contract, or because of its execution or attempted execution, or because of any breach hereof.

43) MODIFICATION OF CONTRACT

No change in or modification, termination or discharge of this Contract, in any form whatsoever, shall be valid or enforceable unless it is in writing and signed by the party to be charged therewith or his duly authorized representative, provided, however, that any change in or modification, termination or discharge of this Contract expressly provided for in this Contract shall be effective as so provided.

44) TRASH REMOVAL

The Contractor shall remove daily from the Facility by means provided by the Contractor all garbage, debris and other waste material (solid or liquid) arising out of or in connection with its operations hereunder, and any such garbage, debris and other waste material not immediately removed shall be temporarily stored in a clear and sanitary condition, approved by the Manager of the Facility, and shall be kept covered except when filling or emptying them. The Contractor shall exercise care in removing such garbage, debris and other waste materials from the Facility. The manner of such storage and removal shall always be subject in all respects to the continual approval of the Port Authority. No equipment or facilities of the Port Authority shall be used in such removal unless with its prior consent in writing. No such garbage, debris or other waste materials shall be or be permitted to be thrown, discharged or disposed into or upon the waters at or bounding the Facility.

45) ENTIRE AGREEMENT

This Contract including the Request for Proposals for # _____ (including its Scope of Work and other attachments, endorsements and exhibits, if any,) as well as the Proposal submitted by the Contractor contains the entire agreement between the parties. In the event of any inconsistency between this Contract and other attachments, endorsements and exhibits, if any, including the Proposal submitted by the Contractor, this Contract shall be controlling.

46) ESCROW AGREEMENT

The Contractor shall archive software and other materials as required in Attachment N, Escrow Agreement.

Parking Access and Revenue Control System—Design, Installation & Maintenance

Attachment C1
Contract Specific Terms and Conditions

1) GENERAL AGREEMENT

Subject to all of the terms and conditions of this Contract, the undersigned (hereinafter called Contractor) hereby offers and agrees to provide all the necessary labor, supervision, personnel, equipment, materials and all other things necessary to perform the work required by this Contract, as set forth in the Scope of Work (Attachment D), and do all other things necessary or proper therefor or incidental thereto, all in strict accordance with the provisions of the Contract and any future changes therein; and the Contractor further agrees to assume and perform all other duties and obligations imposed upon it by this Contract.

In addition, all things not expressly mentioned in the Scope of Work but involved in the carrying out of its intent and in the complete and proper execution of the matters referred to in and required by this Contract are required by the Scope of Work, and the Contractor shall perform the same as though they were specifically delineated, described and mentioned therein.

2) SPECIFIC DEFINITIONS AND ACRONYMS

To avoid undue repetition, the following terms, as used in this Contract, shall be construed as follows:

The term "Director", "General Manager", "Manager", shall mean a Port Authority employee designated by the Port Authority to manage all aspects of this Contractor or his/her successor in duties for this purpose of this Contract, acting personally or through his/her duly authorized representative.

"Contractor" shall mean the Port Authority's Contractor awarded this Contract to provide the specified services under this Contract

"Employees", "Staff" shall refer to employees of the Contractor

"EWR" shall refer to Newark Liberty International Airport

"Facility" or "Facilities" shall mean:

a) John F. Kennedy International (JFK) and LaGuardia (LGA) airports located in the borough and county of Queens in the city and state of New York
b) Newark Liberty International (EWR) Airport in the cities of Newark (Essex County) and Elizabeth (Union County), in the state of New Jersey
c) Stewart International (SWF) Airport located in the county of Orange in the city of Newburgh in the state of New York

"JFK" shall refer to John F. Kennedy International Airport

"Labor" means any Contractor employees directly employed to perform services related to the work described herein. The Manager or his/her designee has the authority to determine what employees of any category are required for "Extra Work" and as to the portion of their time allotted to Extra Work; and "cost of labor" means the wages actually paid to and received by such employees plus a proper proportion of (a) vacation allowances and union dues and assessments which the employer actually pays pursuant to contractual obligation upon the basis of such wages, and (b) taxes actually paid by the employer pursuant to law upon the basis of such wages and workers' compensation premiums paid pursuant to law.

"LGA" shall refer to LaGuardia Airport

"PA" or "Port Authority" or “Authority” shall refer to Port Authority of New York & New Jersey

"SWF" shall refer to Stewart International Airport

3) DESCRIPTION OF SERVICES

Please refer to Attachment D: "Scope of Work" for full description of services required under this Contract.

4) DURATION OF CONTRACT

The term of the Contract (hereinafter called the Initial Term or “Base Term”) is for six (6) year period (the “Initial Term” or “Base Term”) commencing at 12:01 a.m. on the Effective Date (said date and time herein sometimes called "the Commencement Date"), and unless sooner terminated, revoked or extended shall expire 11:59 p.m. on the day before the sixth anniversary of the Effective Date (said date sometimes herein called the ”Expiration Date").

The Port Authority shall have the right to extend this Contract for up to three (3) additional two (2) year periods from the Expiration Date originally fixed herein, upon the same terms and conditions subject only to adjustments of charges, if applicable to this Contract, as may be hereinafter provided in the paragraph entitled “Escalation/Price Adjustment.” If the Port Authority shall elect to exercise the Option(s) to extend this Contract, then, no later than sixty (60) days prior to the Expiration Date, the Port Authority will send a notice that it is extending term of this Contract, and this Contract shall thereupon be extended for the applicable extension period subject only to the adjustment of charges as hereinafter provided.

The Port Authority shall have the absolute right to extend this Contract for an additional one hundred eighty (180) day period subsequent to the Expiration Date hereinbefore established or subsequent to the end of the last exercised option period, if any, subject to the same terms and conditions of the Contract. The charges quoted by the Contractor that

are in effect during the last year of the Initial Term or the last exercised Option Period shall remain in effect during this extension period without escalation. The Port Authority will advise the Contractor, in writing, at least thirty (30) days prior to the Expiration Date of the previous contract period.

5) PAYMENT

The Authority agrees to pay to the Contractor and the Contractor agrees to accept from the Authority as full and complete consideration for the performance by the Contractor, of all its duties and obligations under this Contract and as sole compensation for the Services performed by the Contractor hereunder, a compensation calculated from the services performed and the respective prices inserted by the Contractor in the Cost Proposal, Attachment and accepted by the Port Authority, forming a part of this Contract, subject only to such additions or deductions in the compensation as may be provided for in the sections hereof entitled Extra Work, the Compensation for Extra Work, Work Orders, the Compensation for Work Orders, Net Cost and the Compensation for Net Cost.

The manner of submission of all bills for payment to the Contractor by the Authority for Services rendered under this Contract will be subject to the approval of the Contract Manager in all respects, including, but not limited to, format, breakdown of items presented and verifying records. All computations made by the Contractor and all billing and billing procedures shall be done in conformance with the following:

a) Payment for new PARCS installations will be made in accordance with the prices applicable to the Milestones that appear below, as accepted by the Authority, as same may have been adjusted hereunder minus any deductions for services not performed and/or any applicable liquidated damages. All Services must be completed within the time frames specified or as designated by the Contract Manager. The Contractor will be due payment only upon acceptance of each deliverable by the Authority. Milestone payments can be invoiced immediately after the milestone has been achieved. Invoice must show the Contractor's Federal Tax Identification Number. Payment will be made within thirty (30) days of Authority verification of the invoice. No certificate, payment, acceptance of any Services or any other act or omission of any representative of the Authority shall operate to release the Contractor from any obligation under or upon this Contract, or to stop the Authority from showing at any time that such certificate, payment, acceptance, act or omission was incorrect or to preclude the Authority from recovering any monies paid in excess of those lawfully due and any damage sustained by the Authority.

The Contractor shall submit all invoices to the following:

The Port Authority of New York and New Jersey
Peter Carbonaro
Aviation Department

Four World Trade Center
150 Greenwich St, 18TH Floor
New York, NY 10006

b) Payments for Maintenance of both the existing PARCS and, when applicable, the new PARCS during the Base Period and Option Years, if exercised by the Authority, shall be a monthly lump sum cost equal to one twelfth (1/12) the annual Maintenance cost in the Contractor's Cost Proposal. Maintenance costs should include all necessary software licensing costs.

c) In the event an audit of received invoices indicates that the correct sum due the Contractor for the relevant billing period is less than the amount actually paid by the Authority, the Contractor shall pay to the Authority the difference promptly upon receipt of the Authority's statement thereof. The Authority may, however, in its discretion elect to deduct said sum or sums from any subsequent payments payable to the Contractor hereunder.

"Final Payment" as the term is used throughout this Contract, shall mean the final payment made for services rendered in the last month of the Contract Term. However should this Contract be terminated for any reason prior to the last month of the Contract Term, then Final Payment shall be the payment made for services rendered in the month during which such termination becomes effective. The Contractor's acceptance of any payment, including Final Payment, shall act as a full and complete release to the Authority of all claims of and of all liability to the Contractor for all things done or furnished in connection with this Contract and for every act and neglect of the Authority and others relating to or arising out of this Contract, including claims arising out of breach of contract and claims based on claims of third persons. No payment, however, final or otherwise shall operate to release the Contractor from any obligations in connection with this Contract.

6) PAYMENT SCHEDULE

To facilitate its performance of the Work under this Contract, the Port Authority Program Manager will authorize the Milestone Payments to be made to the Contractor in accordance with the following milestone payment schedule. The percentages set forth below shall be applied to the difference of the Total Contract Price minus the lump sum amount for maintenance of the existing and new systems.

JFK Milestone Payment Schedule

Milestone Payment	*Percent Total of Price*	*Cumulative Percentage*
10% upon submission and acceptance of the Critical Design Review*	10%	10%
10% upon successful completion of the Factory Acceptance Test**	10%	20%
15% upon completion of 25% of lanes completing Site Acceptance Testing	15%***	35%
15% upon completion of 50% of lanes completing Site Acceptance Testing	15%	50%
20% upon completion of 75% of lanes completing Site Acceptance Testing	20%	70%
20% upon completion of 100% of lanes completing Site Acceptance Testing and 100% of Pay-On-Foot Machines being installed and tested	20%	90%
5% upon completion of Operational Acceptance Test	5%	95%
5% upon completion of Final System Acceptance at all four airports	5%	100%

*A single Critical Design Review for the entire four-airport PARCS contract is expected.
**A single Factory Acceptance Test for the entire four-airport PARCS contract is expected.
***This amount shall include costs for the requisite training programs, as outlined in Attachment D, Scope of Work.

EWR Milestone Payment Schedule

Milestone Payment	*Percent Total of Price*	*Cumulative Percentage*
10% upon submission and acceptance of the Critical Design Review*	10%	10%
10% upon successful completion of the Factory Acceptance Test**	10%	20%
15% upon completion of 25% of lanes completing Site Acceptance Testing	15%***	35%
15% upon completion of 50% of lanes completing Site Acceptance Testing	15%	50%
20% upon completion of 75% of lanes completing Site Acceptance Testing	20%	70%
20% upon completion of 100% of lanes completing Site Acceptance Testing and 100% of Pay-On-Foot Machines being installed and tested	20%	90%
5% upon completion of Operational Acceptance Test	5%	95%
5% upon completion of Final System Acceptance at all four airports	5%	100%

*A single Critical Design Review for the entire four-airport PARCS contract is expected.
**A single Factory Acceptance Test for the entire four-airport PARCS contract is expected.
***This amount shall include costs for the requisite training programs, as outlined in Attachment D, Scope of Work.

LGA Milestone Payment Schedule

Milestone Payment	*Percent Total of Price*	*Cumulative Percentage*
10% upon submission and acceptance of the Critical Design Review*	10%	10%
10% upon successful completion of the Factory Acceptance Test**	10%	20%
15% upon completion of 25% of lanes completing Site Acceptance Testing	15%***	35%
15% upon completion of 50% of lanes completing Site Acceptance Testing	15%	50%
20% upon completion of 75% of lanes completing Site Acceptance Testing	20%	70%
20% upon completion of 100% of lanes completing Site Acceptance Testing and 100% of Pay-On-Foot Machines being installed and tested	20%	90%
5% upon completion of Operational Acceptance Test	5%	95%
5% upon completion of Final System Acceptance at all four airports	5%	100%

*A single Critical Design Review for the entire four-airport PARCS contract is expected.
**A single Factory Acceptance Test for the entire four-airport PARCS contract is expected.
***This amount shall include costs for the requisite training programs, as outlined in Attachment D, Scope of Work.

SWF Milestone Payment Schedule

Milestone Payment	*Percent Total of Price*	*Cumulative Percentage*
10% upon submission and acceptance of the Critical Design Review*	10%	10%
10% upon successful completion of the Factory Acceptance Test**	10%	20%
30% upon completion of 50% of lanes completing Site Acceptance Testing	30%***	50%
30% upon completion of 100% of lanes completing Site Acceptance Testing and 100% of Pay-On-Foot Machines being installed and tested	30%	80%
15% upon completion of Operational Acceptance Test	15%	95%
5% upon completion of Final System Acceptance at all four airports	5%	100%

*A single Critical Design Review for the entire four-airport PARCS contract is expected.
**A single Factory Acceptance Test for the entire four-airport PARCS contract is expected.
***This amount shall include costs for the requisite training programs, as outlined in Attachment D, Scope of Work.

7) ESCALATION/PRICE ADJUSTMENT

All Contract prices for maintenance labor and parts and for extra work labor and parts shall be applicable through the end of the Base Term. The Contractor's compensation for the Option Periods shall be adjusted as stated below, but shall not exceed three (3%) percent per year of the Option Periods:

a) For the first year of the first two-year Option Period of the Contract, the quarterly United States Bureau of Labor Statistics Employment Cost Index for Wages and Salaries for Private Industry Workers Professional, Specialty and Technical (non seasonally adjusted data June 1989 = 100) (hereinafter the "Index") for the second Quarter of 2021 and second Quarter of 2022 shall be obtained. The compensation for services and Extra Work labor payable in the sixth year of the Base Term of the Contract shall be multiplied by a fraction, the numerator of which shall be said Index for the second Quarter of 2021 and the denominator of which shall be said Index for the second Quarter of 2022. The resulting product shall be the compensation payable for services and Extra Work labor in the first year of the first Option Period.

b) For the second year of the first Option Period, the Index for the second Quarter of 2023 shall be obtained. The compensation for services and for Extra Work labor payable in the second year of the option period shall be the Prices payable in the first year of the option period multiplied by a fraction, the numerator of which shall be said Index for the second Quarter of 2023 and the denominator of which shall be the number of said Index for the second quarter of 2022. The resulting product shall be the compensation payable for services and Extra Work labor in the second year of the first Option Period.

c) For the first year of the second Option Period, the Index for the second Quarter of 2024 shall be obtained. The compensation for services and for Extra Work labor payable in the first year of the second option period shall be the Prices payable in the second year of the first option period multiplied by a fraction, the numerator of which shall be said Index for the second Quarter of 2024 and denominator of which shall be the number of said Index for the second Quarter 2023. The resulting product shall be the compensation payable for services and Extra Work labor in the first year of the second Option Period.

d) For the second year of the second Option Period, the Index for the second Quarter of 2025 shall be obtained. The compensation for the services and for Extra Work labor payable in the second year of the second option period shall be the Prices payable in the first year of the second option period multiplied by a fraction, the numerator of which shall be said Index for the second Quarter 2025 and the denominator of which shall be the number of said Index for the second Quarter of 2024. The resulting product shall be the compensation payable for services and Extra Work labor in the second year of the second Option Period.

e) For the first year of the third Option Period, the Index for the second Quarter of 2026 shall be obtained. The compensation for services and for Extra Work labor payable in the first year of the second option period shall be the Prices payable in the second year of the first option period multiplied by a fraction, the numerator of which shall be said Index for the second Quarter of 2026 and denominator of which shall be the number of said Index for the second Quarter 2025. The resulting product shall be the compensation payable for services and Extra Work labor in the first year of the third Option Period.

f) For the second year of the third Option Period, the Index for the second Quarter of 2027 shall be obtained. The compensation for the services and for Extra Work labor payable in the second year of the second option period shall be the Prices payable in the first year of the second option period multiplied by a fraction, the numerator of which shall be said Index for the second Quarter 2027 and the denominator of which shall be the number of said Index for the second Quarter of 2026. The resulting product shall be the compensation payable for services and Extra Work labor in the second year of the third Option Period.

g) In the event of a change of the basis for the computation of the said Index or the discontinuance of its publication, such other appropriate index shall be substituted as may be agreed upon by the Authority and the Contractor as properly reflecting changes in the value of the of the services and Extra Work labor similar to that established in the said Index. If the parties cannot agree, the Authority will select the substitute index.

The Contractor's compensation for Services and Extra Work labor for the 180-day extension option shall not be subject to adjustment. Labor and service costs for the 180-day extension period shall be the same as in effect during the year prior to the start of the 180-day option.

8) HOLIDAYS

The following holidays will be observed at the Site of the Work:

New Year's Day
Martin Luther King Day
President's Day
Memorial Day
Independence Day
Labor Day
Columbus Day
Veteran's Day
Thanksgiving Day
Day after Thanksgiving
Christmas Day

and such other days as may be declared holidays by the legislature of the state in which the work is to be performed. This list is subject to periodic revision and the Contractor shall be responsible for obtaining all updated lists from the Port Authority Manager.

No work shall be performed on a holiday without the Port Authority's Manager's approval. The Port Authority reserves the right to order work on a Holiday.

Contractor employees who work directly under this Contract shall not receive additional compensation for services provided on a Holiday.

9) EXTRA WORK

Except as specifically hereinafter provided in this numbered clause, the Contractor shall immediately supply such modified or additional products and services as the Authority may direct ("Extra Work"). Unless such changes or additions are made due to fault on his part, or on the part of others performing on behalf of the Contractor whether or not in privity of contract with the Contractor, and if the Contractor incurs additional costs solely as a result of such changes and additions, the Contractor may request compensation for such additional costs in addition to the compensation provided for elsewhere in this Contract. Agreement by the Authority, if such is forthcoming, shall be in writing. The execution of the aforementioned written agreement shall be a condition precedent to payment of any additional compensation for changes or additions. Accordingly, if the Authority directs the Contractor to make any change in or addition to products or services which entitle him to compensation in addition to that provided for elsewhere herein, he shall not proceed with such changes or additions prior to execution of the aforementioned written agreement except as set forth in the clause hereof entitled "Compensation for Extra Work".

If, as a result of any changes in or additions to the products or services the Authority directs the Contractor to make, the costs of performance of his obligations hereunder are decreased, the parties agree to make such adjustments by way of reduction in the compensation provided for elsewhere herein as they may deem equitable and reasonable and, in making such adjustments, no allowance shall be made for anticipated profits.

The Director shall have the authority to order Extra Work up to an amount equal to six percent (6%) of the Total Estimated Price for the Base Term plus that for any option periods that have been exercised unless the Contractor is advised of a greater authorization in a letter signed by the Authority's Director of Procurement. Nothing herein shall be construed as a representation that any changes or additions will be ordered.

10) COMPENSATION FOR EXTRA WORK

The Director and the Contractor may agree, in writing, on lump sum or other compensation for Extra Work. For Extra Work activities that involve the addition of an entry or exit lane or

the addition of a Pay-on-Foot Machine, costs referenced in Cost Per Lane (Attachment C2, Payment Sheet 3) shall be used for all equipment in the lane. For Extra Work activities that involve the replacement or addition of specific equipment, costs referenced in Sample Replacement Equipment Price List for New PARCS (Attachment C2, Payment Sheet 4) shall be used. In the event that no such agreement is reached compensation shall be increased by the sum of the following amounts and such amounts only:

a) for labor, the applicable hourly rates for extra work set forth in the Cost Proposal, as accepted by the Authority;
b) the actual net cost in money of the materials required for the Work; and
c) in addition to the foregoing, if the Extra Work is performed by a subcontractor, five percent (5%) of the amounts under (A) and (B). No Extra Work shall be performed by a subcontractor without the prior written approval of the Authority.

11) EXTRA WORK PROCEDURES

Whenever any Extra Work is performed by the Contractor on a basis other than on a lump sum basis, the Contractor shall, as a condition precedent to payment for such work, furnish to the Director or her authorized representative at the end of each day daily time slips showing (a) the name and employee number of each person employed thereon, and the number of hours in each day during which they performed Extra Work; (b) a brief description of the nature of the work performed and a list of material and equipment used and the Port Authority authorized representative who approved the Extra Work. Item (b) shall be supplemented by the Contractor at a later date with a statement indicating from whom materials were purchased and the amount paid therefor. Such daily time slips are for the purpose of enabling the Director or her authorized representatives to determine the accuracy of the amounts claimed by the Contractor.

12) PERFORMANCE OF EXTRA WORK

The provisions of this Contract relating generally to the Work shall apply without exception to any Extra Work required and to the performance thereof, except to the extent that a written order in connection with any particular item of Extra Work may expressly provide otherwise.

13) WORK ORDERS

The Contractor shall provide changes to the PARCS System and its components when requested in writing by the Authority via the Work Order process. Work Orders may include work ranging in scope from minor system updates up to the design and implementation of major System changes, such as equipment installation or system enhancements requiring the integration of new technologies and operational procedures. For Work Order activities that involve the addition of an entry or exit lane or the addition of a Pay-on-Foot Machine, costs referenced in Payment Sheet 3 (Attachment C2) shall be used for all equipment. For

Work Order activities that involve the replacement or addition of specific equipment, costs referenced in Sample Replacement Equipment Price List for New PARCS (Attachment C2, Payment Sheet 4) shall be used.

14) COMPENSATION FOR WORK ORDERS

The Director and the Contractor may agree, in writing, on lump sum or other compensation for Work Orders. In the event that no such agreement is reached compensation shall be increased by the sum of the following amounts and such amounts only:

a) for labor, the applicable hourly rates for extra work set forth in the Cost proposal, as accepted by the Authority;
b) the actual net cost in money of the materials required for the Work; and
c) in addition to the foregoing, if the Work Order is performed by a subcontractor, five percent (5%) of the amounts under (A) and (B). No Work Orders shall be performed by a subcontractor without the prior written approval of the Authority.

15) WORK ORDER PROCEDURES

In response to the Authority's request for System changes, the Contractor shall submit a Work Order proposal, that includes, at a minimum, the following information:

a) Detailed Description of Work, indicating the deliverables, description of the work efforts involved, including testing, resources required to perform the work and impact to System operation and availability;
b) Detailed assumptions as to what is required from or to be provided by the Port Authority;
c) Detailed breakdown of all labor required, by category of personnel, and explanation of the work to be performed by that staff;
d) Detailed schedule, indicating activity milestones with associated completion dates;
e) Detailed resource schedule including the names of Contractor staff, number of hours per day and the dates each resource is required;
f) Detailed list of materials, supplies or equipment that will be required to complete the Work Order;
g) Description of any changes to either the maintenance plan/schedule or approved installation plan/schedule of the new PARCS as a result of the Work Order, if any. Indicate addition/deletion of specific items in the monthly maintenance plan and any increment/decrement of monthly maintenance costs;
h) Statement of warranty; and
i) Pricing summary

16) PERFORMANCE OF WORK ORDERS

All work shall be performed in accordance with the terms and conditions of the Contract.

Written approval with written direction to proceed by the Port Authority Project Manager of Work Order proposals submitted by the Contractor, shall constitute an agreed-to Work Order under this agreement, subject to the terms and conditions of the Contract. Preparation of the Work Order proposal shall not be a compensable service under this agreement.

a) Delays in Completion of an Approved Work Order

The Contractor shall adhere to the schedule set forth in each Work Order. Damages for delay of work shall follow the schedule for Liquated Damages of comparable items stated in the Contract, unless it can be demonstrated that the Contractor is not at fault for the delay. Any additional Liquidated Damages with regard to Work Orders shall be agreed upon between the Contractor and the Port Authority during the Work Oder proposal phase. In such cases, the Contractor shall give written notice to the Authority's Project Manager of any delay within two days from the beginning thereof, and its failure so to do shall constitute a waiver of any extension of time therefor. Time is of the essence of the Contractor's obligations hereunder.

b) Certification of Completion

Upon the satisfactory inspection/testing and completion of all work whatsoever required under each Work Order to the Authority's satisfaction, the Contractor shall submit to the Authority a certificate in writing stating completion of the work for Authority approval. The certificate of completion shall include all information as the Authority's Project Manager may require (including, but not limited to (i) certification to the Authority in writing that he has paid and caused his subcontractors to pay at least the prevailing rate of wage and supplements required by the Contract and (ii) a detailed, sworn statement of all claims and demands, just or unjust, of materialmen, subcontractors, laborers and third persons then outstanding and/or which he has reason to believe may thereafter be made, (iii) a certificate in writing stating the total compensation earned under the Work Order and (iv) approved test results. Within thirty days after receipt of the above, and agreement by the Authority of the satisfactory completion of the work, the Authority shall pay to the Contractor by check the amount so certified by the Contract Manager, minus all prior payments and advances to or for the account of the Contractor, if any under the Work Order. The Contractor's acceptance of the final payment under this Contract shall operate as a release to the Authority of all claims of and of all liability to the Contractor for all things done or furnished by the Contractor and for every act and neglect of the Authority and for every act and neglect of the Port Authority and others relating to or arising out of this Contract, including claims arising out of breach of contract and claims based on claims of third persons. No payment, however, final or otherwise shall operate to release the Contractor from any obligations in connection with this Contract..

c) Performance of Services

The Authority's Project Manager shall have authority to increase, decrease and modify the work and may suspend performance of any work for any period during which he/she deems it undesirable to proceed therewith for any reason, whether or not either of the parties is responsible for such reason; and may cancel any Work Order as to any work not yet performed if deemed undesirable to proceed therewith for any reason, without prejudice to rights and obligations arising out of work already performed. The Authority is only obliged to compensate the Contractor for work that is completed to the satisfaction of the Authority's Project Manager.

The Contractor shall, within twenty-four (24) hours, comply with any oral or written requests given by the Authority's Project Manager to correct or remedy a condition or situation deemed by the Authority to require action. These requests will address conditions that threaten the safety of people, the facilities or the system availability. Immediate response shall be expected of the Contractor's personnel for any condition or situation determined by the Authority to constitute any emergency. Contractor shall submit to the Authority's Project Manager on the first day of each calendar month during the term of this Contract a written report setting forth the actions taken by the Contractor with respect to any matters which the Project Manager may have, during the preceding month, requested the Contractor to correct or remedy.

d) Work Order Warranty

The Contractor shall warrant all work performed as part of an approved Work Order against defects in material and workmanship for a period of at least twelve (12) months following the Authority's approval of the Issuance of the Certificate of Completion. Proposer shall provide detail concerning its warranty coverage in its Proposal.

During the Work Order Product Warranty Period, commencing with the acceptance day of the approved Testing, the Contractor shall provide Warranty Service, at no cost to the Port Authority, on all equipment and software furnished under the Contract such that the Work Order Product will perform in accordance with the specifications as defined and specified in the Contractor's Work Order (the "Specifications"), twenty-four (24) hours a day, seven (7) days a week, including Holidays. Such performance of the features and functions implemented as part of the Work Order shall be referred to as performing in "Working Order". During such a period, the Contractor is expected to provide a Warranty Service that shall include: on-site diagnosis and repair of defects in the equipment and software furnished herein; as well as technical support regarding the operational use of the features and functions provided as part of the Work Order.

e) Work Order Testing

As part of the Work Order proposal, the Contractor shall prepare and deliver to the Authority a comprehensive Acceptance Test Plan that describes all the activities and

tasks associated with testing of the Work of the individual Work Order. At a minimum, the Contractor's Acceptance Test Plan shall comply with the requirements for Factory, Field, Site and Operational testing specified in the Contract, unless the Contractor can demonstrate that the requirements for testing do not apply for the work performed in the specific Work Order.

17) NET COST WORK

Net Cost Work shall be paid in addition to Extra Work compensation and shall be computed in the same manner as Extra Work, including any percentage addition to cost as set forth in Section 9 Extra Work Compensation (above). Performance of such Net Cost Work shall be subject to all provisions of the Contract relating to performance of Extra Work. Compensation for said Net Cost Work shall not be charged against the total amount of compensation authorized for Extra Work.

18) INCREASE AND DECREASE IN SERVICES, AREAS OR FREQUENCIES

The Director shall have the right, at any time and from time to time in his sole discretion, to increase and/or decrease the services required hereunder, frequencies of all or any part of the services required hereunder or to add areas not described herein in the Specifications or remove areas or parts of areas, which are hereunder so described. In the event the Superintendent/Manager decides to change any frequencies or areas such change shall be by written notice not less than 24 hours, said changes to be effective upon the date specified in said notice.

In the event of an increase or decrease in services, areas or frequencies, the Contractor’s compensation will be adjusted to reflect such change in areas or frequencies utilizing the applicable hourly rates for such services (for the applicable Contract year) as set forth on the Authority-accepted Cost Proposal.

Where no specific Unit Price has been quoted for the type of services to be increased or decreased, the Manager shall have the right to negotiate the compensation to reflect such change, whether an increase or decrease in areas or frequencies, which, in the opinion of the Manager, are necessary to complete the work, by multiplying the increased or decreased amount by the negotiated rate.

In the event of a decrease in services, the Contractor shall not be entitled to compensation for Work not performed.

No such changes in areas or frequencies will be implemented which results in a total increase or decrease in compensation that is greater than 50% of the Total Estimated Contract Price for the Base Term or, if changes are to be implemented during an Option Period, 50% for that Option Period.

Any increases in frequencies or areas shall not constitute Extra Work and, as such, shall not be limited by the Extra Work provisions of this Contract.

19) LIQUIDATED DAMAGES

The Contractor's obligations for the performance and completion of the Work within the time or times provided for in this Contract are of the essence of this Contract. In the event the Contractor fails to satisfactorily perform all or part of the Work required hereunder in accordance with the requirements set forth in the Scope of Work (as the same may be modified in accordance with the provisions set forth elsewhere herein) then, inasmuch as the damage and loss to the Port Authority for such failure to perform includes items of loss whose amount will be incapable or very difficult of accurate estimation, the damages for such failure to perform shall be liquidated as stated in Attachment D, "Scope of Work", attached, unless delay is not due to the fault of the Contractor.

The Authority's Project Manager shall determine whether the Contractor has performed in a satisfactory manner and his/her determination shall be final, binding and conclusive upon the Contractor. Failure of the Authority's Project Manager or the Port Authority to impose liquidated damages shall not be deemed Port Authority acceptance of unsatisfactory performance or a failure to perform on the part of the Contractor.

Nothing contained in this Section nor the exercise of any right by the Port Authority hereunder shall be deemed to be a waiver or relinquishment by the Port Authority of any other rights it may have hereunder including any right to terminate this agreement based on the Contractor's breach at Law or in equity.

20) PREVAILING WAGES

For the purposes of this Contract, the annual prevailing wage and supplements schedules for the work being performed under this contract in New York City are those published by the Bureau of Labor Law, pursuant to Labor Law §§220 and 230 and New York City Administrative Code §6-109 and located at the New York City Comptroller's website at http://comptroller.nyc.gov/general-information/prevailing-wage/, for the locality and for the period of time in which the work is performed.

For the purposes of this Contract, for work being performed in the State of New Jersey, Contractors and Subcontractors are directed to utilize the State of New Jersey, Department of Labor and Workforce Development prevailing wage levels established pursuant to the New Jersey Prevailing Wage Act (N.J.S.A. 34:11-56.25 et seq.) for workers engaged in public works projects in the Counties of Bergen, Essex, Hudson and Union. The applicable prevailing wage rates shall be those, which are in effect for the locality and for the period of time in which the work is to be performed. Current prevailing wage rates may be

downloaded at:
http://lwd.state.nj.us/labor/wagehour/wagerate/prevailing_wage_determinations.html

For the purposes of this Contract, the annual prevailing wage and supplements schedules for the work being performed under this contract in Orange County are those published by the New York State Department of Labor and located at the New York State's website at https://wpp.labor.state.ny.us/wpp/publicViewPWChanges.do, for the locality and for the period of time in which the work is performed.

The provisions of this clause are inserted in this Contract for the benefit of such workmen, laborer, carpenter or mechanic as well as for the benefit of the Port Authority; and if the Contractor or any subcontractor shall pay or provide any workmen, laborer, carpenter or mechanic less than the rates of wages and supplements above described, such workmen, laborers, carpenters and mechanics shall have a direct right of action against the Contractor or such subcontractor for the difference between the wages and supplements actually paid or provided and those to which they are entitled under this clause. If such workmen, laborer, carpenter or mechanic are employed by any subcontractor whose subcontract does not contain a provision substantially similar to the provisions of this clause (requiring the payment or provision of a least the above minimum, and providing for a cause of action in the event of the subcontractor's failure to pay or provide such wages and supplements) such workmen, laborer, carpenter or mechanic shall have a direct right of action against the Contractor. The Port Authority shall not be a necessary party to any action brought by any workmen, laborer, carpenter or mechanic to obtain a money judgment against the Contractor or any subcontractor pursuant to this clause.

Nothing herein contained shall be construed to prevent the Contractor or any subcontractor from paying higher rates or providing higher supplements than the minimum hereinbefore described; and nothing herein contained shall be construed to constitute a representation or guarantee by the Port Authority that the Contractor or any subcontractor can obtain workmen, laborer, carpenter or mechanic for the minimum hereinbefore described.

The Contractor's or Subcontractor's failure to comply with any provision of this numbered clause may be deemed as a substantial breach of this Contract.

21) MATERIAL, EQUIPMENT AND SUPPLIES

The Contractor will be required to stock, maintain and have quick access to the spare parts and materials, tools or other equipment as may be necessary to make replacements and repairs consistent with the terms described herein. All parts used from said inventory shall be replaced such that the available spare parts remain at a constant quantity suitable for ensuring that the system maintains its mandated availability requirements. The Contractor shall be required to inspect inventoried spare parts on a scheduled basis and assure that these parts are in good working order. The Contractor must maintain an inventory tracking process that provides reporting of inventory items at each storage location, item use

(record of inventory withdrawal, including a cross-reference to the associated service call, work order or preventive maintenance task), required item quantity, current item quantity on hand, item reorder quantity. These records must be available for Authority inspection and validation at all times.

Contractor shall keep a sufficient inventory of spare parts to allow for the replacement of failed components, and components, which in its judgment, need replacement. Components that have been repaired, as opposed to replaced, more than three times shall be replaced at the Authority's option.

Spare parts shall be interchangeable with their corresponding part and equal in quality to original equipment parts. All spare parts shall be reconfigured to the latest revision during the maintenance period. Contractor shall have available at least two sources located in the United States of America (US) for spare parts that are exchanged regularly during preventive maintenance. Contractor shall also endeavor to have other spare parts available from two US sources. A detailed list of all spare parts with manufacturer name, model number, quantities required to be on hand, warranty information must be provided by the Contractor and submitted to the Port Authority Program Manager prior to contract signing.

The Contractor shall be responsible for all equipment provided to it by the Port Authority. If such equipment is damaged or destroyed due to misuse or negligence, then the Contractor may be required to reimburse the Port Authority for the cost or replacement thereof. A tagged inventory register will be maintained by the Contractor on tools and equipment with a unit value in excess of One Hundred Dollars and No Cents ($100.00).

22) DOCUMENTATION

The Contractor shall organize and maintain a library of all system, technical and facility documentation at each of the Airports covered under this contract. This library will include (but not be limited to) all existing manufacturer's documentation, design and construction documentation, third party software documentation, operating manuals and custom documentation developed by the Contractor and others useful in support of the Airport Parking and Revenue Control System. The libraries shall be available and accessible by both Contractor and Authority personnel.

This library shall be maintained both in hardcopy as well as digital format. Facilities shall be available to view electronically stored documents and to duplicate documentation or make hard copies upon request. The Contractor shall maintain an inventory of all documentation in the library and shall inventory the library every six (6) months. Every six (6) months, the Contractor shall review and update the library with available revisions to existing documentation and new documents. Following each inventory review, the Contractor shall provide a report to the Authority on the status of the document inventory at each of the libraries.

The Contractor shall provide updates to any and all existing system and facility documentation (as defined in Part B, Section 6 of this document) or to any documentation provided the Authority by the Contractor in addition to the aforementioned documentation to reflect any changes stemming from Maintenance, Extra Work, Work Order and Net Cost activities. Irrespective of any Maintenance, Extra Work, Work Order and Net Cost activities, where existing documentation is found to be inaccurate or missing, the Contractor must update, replace and or provide such documentation when so directed by the Authority in writing. Updates to documentation stemming from Maintenance and Extra Work activities may not be separately billed to the Authority. Where directed to update, replace or provide documentation independent of Maintenance, Extra Work, Work Order and Net Cost Activities, the Contractor may bill the Authority for such work as Extra Work (see Part A, "Extra Maintenance Work").

23) METHOD OF OPERATION

Contractor shall not be required to install equipment or appurtenances, other than that required for the installation, maintenance and operation of the equipment, without additional compensation therefor. If directed by the Manager to install any such additional equipment or appurtenances, they shall be considered to be Extra Work and the Contractor shall be compensated as set forth in the clause entitled "Compensation for Extra Work," "Compensation for Work Orders," "Compensation for Net Cost".

Contractor does not assume possession of and/or control over any part of the equipment, except to the extent that such possession and/or control are necessary for the purposes of performing its obligations under this Contract. The Authority shall remain the owner of the equipment serviced by the Contractor.

In the event that the Airport Parking and Revenue Control System is not in Working Order, and the Contractor is not meeting the standards of System Availability or the standards of System Performance because of a malfunction which, in the opinion of the Authority, is unlikely to be resolved by the Contractor, the Authority may, at the Contractor's expense, restore the Airport Parking and Revenue Control System to Working Order or provide a work around. Contractor shall credit to the Authority the expenses associated with any third party work up to the Monthly Maintenance Payment.

Any breach of or delay in performing the maintenance obligation required hereunder, which results in or tends to result in a substantial interruption of service, shall be deemed a substantial breach of this Contract entitling the Authority at its option to take over the maintenance either itself or through others, and to collect from the Contractor, the additional costs, if any, of such maintenance or to terminate this Contract without liability to the Contractor; provided that in case of delay beyond the Contractor's control which it is unable to overcome by the exercise of all reasonable efforts or which it could not reasonably have anticipated or avoided, the Contractor shall not be deemed in breach. It shall be deemed that strikes, lockouts, fire, explosion, theft, floods, riots, civil commotion,

war, acts of God and acts of government not yet specifically proposed or taken are beyond the Contractor's control. In case of delays beyond the Contractor's control, the Authority may, at its option and without liability to the Contractor, take over the maintenance either itself or through others until the Contractor resumes performance of the maintenance.

The Contractor shall comply with all provisions of federal, state, municipal, local and departmental laws, ordinances, rules, regulations and orders which would affect the Contract and the performance thereof and those engaged therein if said Contract were being performed for a private corporation, except where stricter requirements are contained herein.

Any assignment or other transfer of this Contract or of any moneys due or to become due hereunder without the written consent of the Authority shall be void and of no effect as to the Authority, except that work may be sublet to such persons as the Program Manager expressly approves in writing. No subcontract shall create any rights against the Authority or relieve the contractor of any obligations, and all subcontractors shall be deemed the Contractor's agents.

The Authority by its officers, employees and representatives shall have the right at all times to examine the supplies, materials, and equipment used by the Contractor and to observe the operations of the Contractor, its subcontractors, agents, servants and employees and to do any act or thing which the Authority may be obligated or have the right to do under this Contract.

Contractor shall pay all duties and imposts, if any, on the importation of any materials used in work under this Contract.

24) TRANSITIONING SERVICES AT START/TERMINATION OF THE CONTRACT

The Contractor shall support an orderly transition from the existing contractor providing maintenance services for the existing PARCS to the new Contract. The Contractor is expected to actively participate in discussions and agree to written plans, which clearly specify the transition period and responsibilities.

25) SITE SPECIFIC RECYCLING AND TRASH REMOVAL

In addition to the trash removal requirements listed in Attachment B, General Contract Provisions, the Contractor is required to properly dispose of any materials, which are considered sensitive, confidential, etc. as outlined in the Port Authority Security Information Handbook. After contract award, the Contractor shall refer to the Port Authority Security Information Handbook for more detailed Protected Information disposal procedures.

Parking Access and Revenue Control System—Design, Installation & Maintenance

Attachment C2
Cost Proposal

ATTACHMENT C2: COST PROPOSAL

1. Total Cost for New PARCS Equipment, Including Design and Installation of New System and Removal of Existing System

Below costs should include all costs associated with tasks outlined in the Attachment D, Scope of Work sections 1.1 and 1.3.

Description	Facility	Cost Per Facility
80 - Entrance and Exit Lanes 65- Pay on Foot Machines (50 CC Only – 15 CC & Cash)	JFK	$_____
40 - Entrance and Exit Lanes. 40 – Pay on Foot Machines (30 CC Only-10 CC & Cash)	LGA	$_____
80 - Entrance and Exit Lanes 65 – Pay on Foot Machines (55 CC Only -10 CC & Cash)	EWR	$_____
16 - Entrance and Exit Lanes 5 - Pay on Foot Machines (All 5 Accepting CC & Cash)	SWF	$_____

Total Cost for All New PARCS Equipment including design and installation at airports listed above:

$_____

Note: Payments for Equipment and Installation will be made in “Milestones Payments” found in Attachment C section 5 titled “Payment”.

2. Annual Cost for Preventative and Remedial Maintenance of Existing and New PARCS Equipment

Below costs should include all costs associated with tasks outlined in the Attachment D, Scope of Work Section 8, PARCS MAINTENANCE.

Included in below figures should be:

Preventative and Remedial Maintenance Labor and Parts for the Existing and New PARCS

System Updates for the Existing and New PARCS

All Software Updates for the New PARCS

Facility	Year 1 Price	Year 2 Price	Year 3 Price	Year 4 Price	Year 5 Price	Year 6 Price	Grand Total for six years
JFK							
LGA							
EWR							
SWF							
Grand Total							

Note: Annual price will be paid in 12 monthly payments by each facility.

3. Fees and Charges

Below costs should include any fees and charges that will occur to the Port Authority that are not already included in Sheet 1, Total Cost for New PARCS Equipment, Including Design and Installation of New System and Removal of Existing System and Sheet 2, Annual Cost for Preventative and Remedial Maintenance of Existing and New PARCS Equipment. Blank lines are available for a listing of other fees not yet mentioned that will be charged to the Port Authority.

Title	Summary	Fee	Estimated Cost for Base Term of Contract
Integration Fee	Cost to integrate third party systems and software		
Credit Card Payment Processing Fee	Per transaction fee to process credit card payments		
Online Prebooking Processing Fee	Per transaction fee to process online prebooking payments		

4. Cost per Lane

Over the course of this Contract, airport redevelopment activities will necessitate the creation of new entry and exit plazas as well as the placement of additional Pay-on-Foot machines. Proposers shall provide the cost for equipment, including installation costs. The costs shall remain in effect for the initial Base Term of the Contract and will increase by the same percentage as maintenance costs during the three two-year Option Periods, if exercised, per Price Adjustment in Attachment C. Costs should cover the maximum functionality for each item as defined in Attachment D, "Scope of Work" and Attachment E, "Functional Requirements".

Cost Per Item:	JFK	LGA	EWR	SWF
Entry Lane				
Exit Lane				
Pay-on-Foot Machine				

5. Sample Replacement Equipment Price List for New PARCS

Proposers shall provide the cost for the equipment listed below. The costs shall remain in effect for the initial Base Term of the Contract and will be increased by the same percentage as maintenance costs during the three two-year Options Periods, if exercised, per Price Adjustment in Attachment C1.

Blank Spaces Provided Below For Additional Replacement Components – to be filled in by Proposers, as necessary. Use additional sheets, as needed.

PARCS Equipment Component	Manufacturer	Unit Price
Ticket Issuing Machine (TIM)		
Cashier Terminal (CT)		
PosiDrive Parking Gate		
Uninterruptable Power Supply (UPS)		
VMS – Fee Display		
Overhead *E-ZPass® Plus™* Antenna		
EZ Pass Plus Patch Antenna		
Credit Card Reader		

ATTACHMENT C2: COST PROPOSAL

Ticket Reader		
LPR Camera		
Backup Tape Drives		
Proximity Card Reader		

5. Staff Pricing for Work Orders, Extra Work & Net Cost

UNIT PRICING for STAFF CATEGORIES FOR WORK ORDERS, EXTRA WORK & NET COST DURING CONTRACT **YEAR 1**				
Personnel Title		Estimated Number of Hours – Only to be used to Compare Proposed Hourly Rates (See Note 1) A	Hourly Rates (See Note 2) B	Extended Total A*B
Project Manager		400	$	$
Professional Engineer		100	$	$
Electrical Engineer		100	$	$
Network Engineer		150	$	$
Licensed Electrician		400	$	$
Senior Technician		250	$	$
Field Technician		1000	$	$
Systems Designer/Engineer		400	$	$
Computer Programmer/Analyst		1000	$	$
Application Specialist		400	$	$
Web Application Programmer		50	$	$
System Integration Specialist		100	$	$
Manufacturer Technician Support		250	$	$
Data Base Administrator		200	$	$
Data Base Programmer		500	$	$
Contract Administrator		100	$	$
(See Note 3 Below)				
Extended Labor Total (Sum of Extended Totals for Each Labor Category)				$

Notes:
Only hours agreed upon for Work Orders, Extra Work and Net Cost projects will be paid.
Hourly Rates are not subject to any additional markup or overhead and prevailing wages should be used, where applicable.
The Contractor shall include/substitute any additional labor categories of staff that may be used in performance of the Contract, and indicate their fixed hourly rates.

ATTACHMENT C2: COST PROPOSAL

UNIT PRICING for STAFF CATEGORIES FOR WORK ORDERS, EXTRA WORK & NET COST DURING CONTRACT **YEAR 2**				
Personnel Title		Estimated Number of Hours – Only to be used to Compare Proposed Hourly Rates (See Note 1) A	Hourly Rates (See Note 2) B	Extended Total A*B
Project Manager		400	$	$
Professional Engineer		100	$	$
Electrical Engineer		100	$	$
Network Engineer		150	$	$
Licensed Electrician		400	$	$
Senior Technician		250	$	$
Field Technician		1000	$	$
Systems Designer/Engineer		400	$	$
Computer Programmer/Analyst		1000	$	$
Application Specialist		400	$	$
Web Application Programmer		50	$	$
System Integration Specialist		100	$	$
Manufacturer Technician Support		250	$	$
Data Base Administrator		200	$	$
Data Base Programmer		500	$	$
Contract Administrator		100	$	$
(See Note 3)				
Extended Labor Total (Sum of Extended Totals for Each Labor Category)				$

Notes:

Only hours agreed upon for Work Orders, Extra Work and Net Cost projects will be paid.

Hourly Rates are not subject to any additional markup or overhead and prevailing wages should be used, where applicable.

The Contractor shall include/substitute any additional labor categories of staff that may be used in performance of the Contract, and indicate their fixed hourly rates.

ATTACHMENT C2: COST PROPOSAL

UNIT PRICING for STAFF CATEGORIES FOR WORK ORDERS, EXTRA WORK & NET COST DURING CONTRACT **YEAR 3**				
Personnel Title		Estimated Number of Hours – Only to be used to Compare Proposed Hourly Rates (See Note 1) A	Hourly Rates (See Note 2) B	Extended Total A*B
Project Manager		400	$	$
Professional Engineer		100	$	$
Electrical Engineer		100	$	$
Network Engineer		150	$	$
Licensed Electrician		400	$	$
Senior Technician		250	$	$
Field Technician		1000	$	$
Systems Designer/Engineer		400	$	$
Computer Programmer/Analyst		1000	$	$
Application Specialist		400	$	$
Web Application Programmer		50	$	$
System Integration Specialist		100	$	$
Manufacturer Technician Support		250	$	$
Data Base Administrator		200	$	$
Data Base Programmer		500	$	$
Contract Administrator		100	$	$
(See Note 3)				
Extended Labor Total (Sum of Extended Totals for Each Labor Category)				$

Notes:
Only hours agreed upon for Work Orders, Extra Work and Net Cost projects will be paid.
Hourly Rates are not subject to any additional markup or overhead and prevailing wages should be used, where applicable.
The Contractor shall include/substitute any additional labor categories of staff that may be used in performance of the Contract, and indicate their fixed hourly rates.

ATTACHMENT C2: COST PROPOSAL

UNIT PRICING for STAFF CATEGORIES FOR WORK ORDERS, EXTRA WORK & NET COST DURING CONTRACT **YEAR 4**				
Personnel Title		Estimated Number of Hours – Only to be used to Compare Proposed Hourly Rates (See Note 1) A	Hourly Rates (See Note 2) B	Extended Total A*B
Project Manager		400	$	$
Professional Engineer		100	$	$
Electrical Engineer		100	$	$
Network Engineer		150	$	$
Licensed Electrician		400	$	$
Senior Technician		250	$	$
Field Technician		1000	$	$
Systems Designer/Engineer		400	$	$
Computer Programmer/Analyst		1000	$	$
Application Specialist		400	$	$
Web Application Programmer		50	$	$
System Integration Specialist		100	$	$
Manufacturer Technician Support		250	$	$
Data Base Administrator		200	$	$
Data Base Programmer		500	$	$
Contract Administrator		100	$	$
(See Note 3)				
Extended Labor Total (Sum of Extended Totals for Each Labor Category)				$

Notes:
Only hours agreed upon for Work Orders, Extra Work and Net Cost projects will be paid.
Hourly Rates are not subject to any additional markup or overhead and prevailing wages should be used, where applicable.
The Contractor shall include/substitute any additional labor categories of staff that may be used in performance of the Contract, and indicate their fixed hourly rates.

ATTACHMENT C2: COST PROPOSAL

UNIT PRICING for STAFF CATEGORIES FOR WORK ORDERS, EXTRA WORK & NET COST DURING CONTRACT **YEAR 5**				
Personnel Title		Estimated Number of Hours – Only to be used to Compare Proposed Hourly Rates (See Note 1) A	Hourly Rates (See Note 2) B	Extended Total A*B
Project Manager		400	$	$
Professional Engineer		100	$	$
Electrical Engineer		100	$	$
Network Engineer		150	$	$
Licensed Electrician		400	$	$
Senior Technician		250	$	$
Field Technician		1000	$	$
Systems Designer/Engineer		400	$	$
Computer Programmer/Analyst		1000	$	$
Application Specialist		400	$	$
Web Application Programmer		50	$	$
System Integration Specialist		100	$	$
Manufacturer Technician Support		250	$	$
Data Base Administrator		200	$	$
Data Base Programmer		500	$	$
Contract Administrator		100	$	$
(See Note 3)				
Extended Labor Total (Sum of Extended Totals for Each Labor Category)				$

Notes:

Only hours agreed upon for Work Orders, Extra Work and Net Cost projects will be paid.

Hourly Rates are not subject to any additional markup or overhead and prevailing wages should be used, where applicable.

The Contractor shall include/substitute any additional labor categories of staff that may be used in performance of the Contract, and indicate their fixed hourly rates.

ATTACHMENT C2: COST PROPOSAL

UNIT PRICING for STAFF CATEGORIES FOR WORK ORDERS, EXTRA WORK & NET COST DURING CONTRACT **YEAR 6**				
Personnel Title		Estimated Number of Hours – Only to be used to Compare Proposed Hourly Rates (See Note 1) A	Hourly Rates (See Note 2) B	Extended Total A*B
Project Manager		400	$	$
Professional Engineer		100	$	$
Electrical Engineer		100	$	$
Network Engineer		150	$	$
Licensed Electrician		400	$	$
Senior Technician		250	$	$
Field Technician		1000	$	$
Systems Designer/Engineer		400	$	$
Computer Programmer/Analyst		1000	$	$
Application Specialist		400	$	$
Web Application Programmer		50	$	$
System Integration Specialist		100	$	$
Manufacturer Technician Support		250	$	$
Data Base Administrator		200	$	$
Data Base Programmer		500	$	$
Contract Administrator		100	$	$
(See Note 3)				
Extended Labor Total (Sum of Extended Totals for Each Labor Category)				$

Notes:

Only hours agreed upon for Work Orders, Extra Work and Net Cost projects will be paid.

Hourly Rates are not subject to any additional markup or overhead and prevailing wages should be used, where applicable.

The Contractor shall include/substitute any additional labor categories of staff that may be used in performance of the Contract, and indicate their fixed hourly rates.

6. Parking Space Count System Design and Installation Price Sheet

(The Port Authority may decide not to purchase a PSCS. The below price sheet is for information only until such time that the Port Authority shall exercise the option to design and install a PSCS at the below listed prices.)

See Attachment E Parking Access and Revenue Control System Functional Specifications (Section 1.05 Subparagraph 10.I Parking Space Count System PSCS)

Facility	Number of Garages	Location and Description of Garages	Number of Spaces Per Level	Price Per Garage
JFK	5	Terminals 1 & 2- Green Garage (3 Levels) Note: Green Garage has 2 Entrances on each Level	Green Level 1- 273 Green Level 2 – 343 Green Level 3 – 322 Total Spaces - 938	$_____
		Terminal 4 - Blue Garage (4 Levels)	Blue Level 1- 183 Blue Levels 2,3,4- 258 Total Spaces - 441	$_____
		Terminal 5- Yellow Garage (5 Levels)	Yellow Level 1- 123 Yellow Levels 2,3,4- 240 Yellow Level 5- 230 Total Spaces - 593	$_____
		Terminal 7- Orange Garage (1 Level)	Orange Level 1 - 278	$_____
		Terminal 8 -Red Garage (4 Levels)	Red Level 1- 273 Red Level 2- 347 Red Level 3- 349 Red Level 4- 356 Total Spaces - 1325	$_____

EWR	2	Parking Lot 4 - Garage (5 Levels)	Level 1 – 260 Level 2 - 541 Level 3 - 553 Level 4 - 553 Level 5 - 553 Total Spaces- 2460	$_____
		Terminal C- Garage (3 Levels)	Level 1- 629 Level 2- 801 Level 3- 911 Total Spaces- 2341	$_____
LGA	1	P4 Parking Garage (5 Levels)	Level 1 – 122 Level 2 – 199 Level 3 - 200 Level 4- 200 Level 5- 193 Total Spaces- 914	$_____
		Total Cost Per Airport	JFK EWR LGA Total Cost All Facilities (JFK,EWR,LGA)	$_____ $_____ $_____ $_____

Parking Access and Revenue Control System—Design, Installation & Maintenance

Attachment D
Scope of Work

1) GENERAL SCOPE OF WORK

This Scope of Work (SOW) defines the Contractor's responsibilities, design requirements, integration criteria and maintenance obligations for a fully functional Parking Access and Revenue Control System (PARCS) desired by the Port Authority of New York and New Jersey for John F. Kennedy International Airport, LaGuardia Airport, Newark Liberty International Airport, and Stewart International Airport.

The Contractor shall:

a) Design and install a new PARCS that meets the functional specifications enumerated in Attachment E, "Functional Specifications", to serve parking operations at John F. Kennedy International Airport (JFK), LaGuardia Airport (LGA), Newark Liberty International Airport (EWR) and Stewart International Airport (SWF).
b) Provide services and materials for the maintenance and operation of all Existing PARCS hardware, software and the network communications equipment (at each entry and exit plaza) that constitute the four separate systems currently serving airport parking operations at JFK, LGA, and EWR until the transition to the New PARCS at each airport is fully installed, accepted and fully operational.
c) Decommission and remove Existing PARCS at each airport.
d) Provide scheduled corrective and preventative maintenance and remedial call-in maintenance (with availability of twenty-four hours a day, seven days a week) of all equipment, hardware and software necessary to maintain the operation and use of the New PARCS at JFK, LGA, EWR and SWF.

2) DEFINITIONS

Component— refers to a hardware device or set of devices, and the attendant set of software, firmware, wires and cables that are integrated connected to PARCS.

Contractor – The individual, partnership, firm, or corporation primarily liable for the acceptable performance of the services contracted and for the payment of all legal debts pertaining to the work who acts directly or through lawful agents or employees to complete the work required under this Contract.

Director—the Authority's Aviation Director or his or her designee in duties for purposes of this Contract.

Factory Acceptance Test—a system test that verifies the functional performance of all systems, subsystems and components of the PARCS. Also referred to as FAT.

Lane Acceptance Test—a test of the equipment in a lane after it has been installed to verify that the equipment was not damaged during shipping, was installed properly and functions in accordance with the Contract requirements. Also referred to as LAT.

Project Manager—the Authority's Airport Access Manager or his designee. Also referred to as Manager and Program Manager.

Off-Hours Period of Maintenance—anytime between 11:59 pm and 8:00 am seven days a week and refers to all airports: LaGuardia Airport, John F. Kennedy International Airport, Newark Liberty International Airport and Stewart International Airport. Also referred to as OPM.

Operational Acceptance Test—a test that comprises all equipment, systems and subsystems at an airport performing under actual conditions. Also referred to as OAT.

PARCS—– Parking Access and Revenue Control System, which is a combination of equipment, subsystems, and supporting infrastructure including operational procedures, software, firmware, websites, documentation, etc. that allows an entity to accurately calculate, collect, track, and report revenues for parking within one or more facilities. Also referred to as "System" or "Existing System" (for existing PARCS) or "New PARCS System" (for System to be installed).

Primary Period of Maintenance— anytime between 8:00 am and 11:59 pm seven days a week, and refers to all airports: LaGuardia Airport, John F. Kennedy International Airport, Newark Liberty International Airport and Stewart International Airport. Also referred to as PPM.

Product Warranty Period—period of time in which the Contractor shall maintain, repair or replace out of service equipment at no cost to the Authority.

Project Team—individuals or entities assigned to the effort of the Contractor. Those individuals include, but are not limited to, employees of the Contractor and/or Subcontractors as well as Port Authority personnel and designees.

Site Acceptance Test—a test of each parking lot plaza's equipment installation as a system. Also referred to as a SAT.

Specifications—the detailed definitions, requirements and all other descriptions of the products and/or service required under this Contract.

Subcontractor—anyone who performs work related to the maintenance or work order processing of the Parking Access and Revenue Control System directly or indirectly for or on behalf of the Contractor (and whether or not in privity of Contract with the Contractor), but

shall not include any person who furnished merely his/her own personal labor or his/her own personal services.

Technician—an individual who has formal training and on-the-job experience, and has achieved competence in troubleshooting, repair and maintenance of parking revenue control systems of the type installed at JFK, LGA, EWR and SWF under this contract. Also referred to as Journeyman.

Work Site—John F. Kennedy International Airport (JFK), LaGuardia Airport (LGA), Newark Liberty International Airport (EWR), Stewart International Airport (SWF), 4 World Trade Center (4WTC), New York, NY, Port Authority Tech Center (PATC), Jersey City, NJ and Port Authority Teleport, Staten Island, NY and the vicinity thereof.

3) OVERVIEW OF OPERATING ENVIRONMENT

The existing Parking Access and Revenue Control System (PARCS), manufactured by 3M (previously Federal APD) is in operation at LaGuardia Airport, John F. Kennedy International Airport, Newark Liberty International Airport and is referred to as the ONYX system. The system at Stewart International Airport was also provided by 3M and is a scaled down system referred to as ScanNet. These systems operate independently and each communicates over a separate Cisco Fiber Optic Transmission product, the Sonet LYNX OC-192 System. Specific details regarding the present system may be found in Attachment I, "Background of Existing System."

The Contractor will have end-to-end responsibility for the support of both the Existing and New PARCS, except where specified by the Authority in the RFP.

4) PROJECT DELIVERY

a) Installation & Implementation Schedule

The installation of the New PARCS shall be delivered in four (4) installments related to the four (4) airports. As a guideline, a projected project schedule is provided below. If a Proposer has a more efficient cost-effective development and installation schedule, it should be included in the proposal along with backup information as to why it differs from the Authority's proposed schedule. If the Authority fails to provide infrastructure that is necessary to support the installation and operation of any component of the New PARCS, in accordance with the Contractor's proposed schedule, the Contractor shall not be entitled to any claims for delay of work. If it is necessary, the parties will agree to a revised schedule if there are delays that are no fault of the Contractor.

b) Maintenance of Existing PARCS

The Contractor shall support and maintain the Existing PARCS at EWR, LGA and JFK until the time that the new system is installed and accepted by the Authority. The Contractor shall not be responsible for support and maintenance of the Existing PARCS at SWF.

c) Maintenance of New PARCS

The Contractor shall support and maintain the New PARCS, after installation, at all four (4) airports.

d) Migration of Operations from Existing PARCS to New PARCS

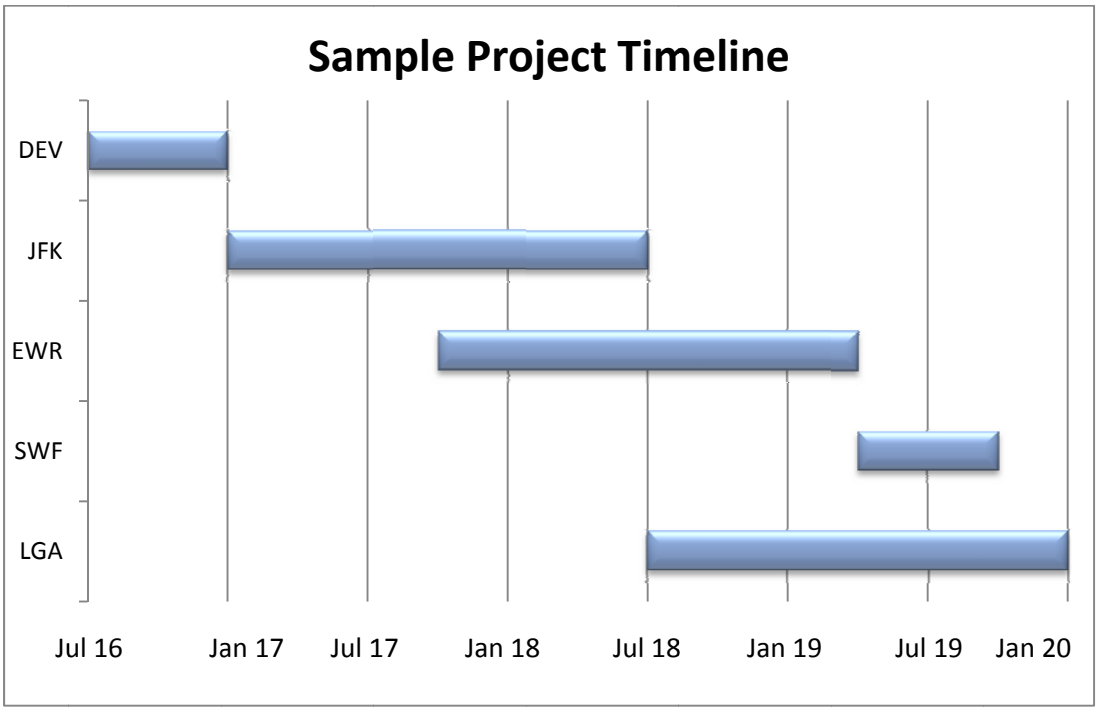
The Contractor shall migrate operations from the Existing PARCS to the New PARCS in a controlled series of phases. During migration, the Contractor shall ensure that the Existing PARCS and the New PARCS continue to operate smoothly and properly without loss of parking spaces or revenue.

At the time of Proposal, the Contractor shall provide a comprehensive detailed phasing plan and methodology to accomplish the following (the "Migration Plan"):

i) Install and test New PARCS Host System;
ii) Convert existing databases and archived data to work with the New PARCS; import data from existing PARCS into New PARCS; Manage database synchronization between the Existing PARCS and the New PARCS until the Existing PARCS is completely decommissioned;
iii) Provide detailed system migration plan addressing infrastructure, network subsystems, communications support, sequence of hardware installations by airport and by lot;
iv) Develop detailed documentation addressing equipment reliability projections, application and systems administration and procedural changes;
v) Ensure that the New PARCS network is functioning 100% to any and all devices including communications concentrators between the host and lane equipment before scheduling migration from existing to new lanes, POF's and servers.
vi) When appropriate and with Authority concurrence, decommission and remove existing communications hardware and servers, in a controlled phased approach, insuring easy fall back to the original system in the event of any migration difficulties;
vii) Provide documentation of all problems and corrective actions that occur while implementing the New PARCS and create a historical database to be used in future development and/or changes to the New PARCS;
viii) Provide documentation identifying any civil work, with timelines, needed to support the functional specifications that are detailed in Attachment E.
ix) Upon removal of Existing PARCS, the Contractor shall provide the Authority with a list of removed equipment. The Authority will review the inventory and provide the Contractor with appropriate disposal instructions.

x) Other items of significance.

This Migration Plan shall also address periods of time/duration during the migration process when components of the existing system may be taken out of service and removed. Upon approval of the Authority such hardware items will be removed by the Contractor and held in inventory at a location provided by the Port Authority for support of the existing system, until such time the existing system is completely decommissioned at all airports.



e) Database Conversion and Synchronization of Existing and New PARCS

The Contractor shall plan, manage, and provide quality assurance of the conversion from the existing databases, communications servers, archived data, data mapping, and any other systems or equipment that shall be replaced as well as synchronize data from the Existing PARCS to the New PARCS. The Contractor shall convert the data from the Existing PARCS into a format that is compatible with the New PARCS and import said data into the New PARCS.

f) Transition Planning from Current Contractor

The Contractor shall support an orderly transition from the existing Contractor providing services to itself. The maximum transition period shall be 180 days, or less, as determined feasible by the Authority. The Contractor shall actively participate in discussions and agree to written plans that are developed by the Authority that clearly specify the transition period and responsibilities.

g) Transition Planning to Future Contractors

The new Contractor shall support an orderly transition to the new maintenance vendor for the maintenance of the PARCS upon completion and termination of the Contract. The maximum transition period shall be 180 days, or less, as determined feasible by the Authority. The Contractor shall actively participate in discussions and agree to written plans that clearly specify the transition period and responsibilities.

5) SYSTEM AVAILABILITY AND RELIABILITY

See Section 12 below for System Availability and Reliability requirements.

6) SYSTEM ADMINISTRATION

The Contractor shall be responsible for cooperating with and assisting when applicable, the Port Authority's third party system administrators for the Existing and proposed New PARCS solution, in accordance with the Harmony clauses in Attachment B, in the Contract.

7) APPLICATION ADMINISTRATION

The Contractor shall be responsible for cooperating with, and assisting when applicable, the Port Authority's third party application administrators for the Existing and proposed New PARCS solution, in accordance with the Harmony clauses in Attachment B, in the Contract.

8) PARCS MAINTENANCE

Primary Period of Maintenance (PPM)—anytime between 8:00am and 11:59pm seven days a week, including holidays.

Off-Hours Period of Maintenance (OPM)—anytime between 11:59pm and 8:00am seven days a week.

a) Maintenance Program

The Contractor shall provide the Port Authority with complete PARCS support for both the Existing and New PARCS systems to comply with the system availability and reliability requirements defined herein. The service coverage for hardware covered by the maintenance contract is twenty-four (24) hours per day, seven (7) days per week, three hundred sixty-five (365) days per year. Contractor-certified technicians shall provide total system support. Access to a Contractor-certified technician includes contact by telephone, e-mail, online problem reporting tools and on-site as needed to provide the levels of support defined within the Contract. The Contractor shall furnish all labor, materials, equipment, travel, supplies, parts, supervision, warning signs, other

safety devices, and all other things necessary or proper for, or incidental to, such maintenance required to maintain and repair all Existing PARCS hardware and all New PARCS hardware installed as part of this project, as well as all PARCS hardware, for both the existing and the new systems during the term of the maintenance portion of this Contract. The scope of the maintenance work includes Preventive Maintenance and Remedial Services Maintenance.

The maintenance program shall be performed to keep the Parking Access and Revenue Control System operating in a proper, safe, and efficient operating condition. Repairs/replacements shall be performed in accordance with the manufacturers written instructions.

The program shall consist of five parts:

i) Preventative Maintenance of the Existing PARCS at EWR, JFK and LGA, as described below
ii) Remedial Maintenance of the Existing PARCS at EWR, JFK and LGA, which consists of service calls from operations personnel and/or Port Authority personnel regarding components of the system not working in accordance with the manufacturer's stated functional and performance specifications regardless of the cause.
iii) Preventative Maintenance of the New PARCS at EWR, JFK, LGA and SWF, as described below
iv) Remedial Maintenance of the New PARCS at EWR, JFK, LGA and SWF, which consists of service calls from operations personnel and/or Port Authority personnel regarding components of the system not working as in accordance with the Contract regardless of the cause.
v) Software Maintenance of the New PARCS at EWR, JFK, LGA and SWF, which consists of maintaining all software furnished, installed and used by the Contractor as described below:

The Authority reserves the right to require the Contractor to utilize specific third party subcontractors where the Authority believes that the successful completion of work is dependent on the skills provided by such resources. At contract commencement, two third parties are engaged in subcontracting services for the PARCS: H&L Electric, and Kapsch TrafficCom. H&L provides on-site technicians for maintenance and remedial repairs of the existing PARCS. Kapsch supplies and maintains the Authority's *E-ZPass® Plus™* equipment.

b) Preventative Maintenance—Existing PARCS

i) The maintenance services to be provided by the Contractor include maintenance for the Existing PARCS hardware and software components used for airport parking operations, and the subsystems, which include, at minimum, the Employee Proximity Access Card System, Automated Vehicle Identification System, License

Plate Recognition System, License Plate Inventory System, Intercom System, *E-ZPass®Plus™*, Credit Card payment middleware and the Parking Space Count System.

ii) The Contractor shall provide resident technicians at EWR, LGA and JFK during the Primary Period of Maintenance (PPM) to maintain the Existing PARCS.

iii) The maintenance performed by the Contractor shall consist of scheduled preventive maintenance of the Existing PARCS at EWR, JFK and LGA, which shall be in accordance with the manufacturer's suggested preventive maintenance recommendations (see Attachment R, Existing System Preventative Maintenance), callback service and engineering updates. Spare parts for the existing system are stored in the storage space provided by the Port Authority at EWR, JFK, LGA and SWF. A recent spare part inventory can be found in Attachment S (Existing System Spare Parts Inventory).

iv) Third party components such as *E-ZPass® Plus*™ equipment and software are to be included in the schedule.

v) The Contractor's staff shall have appropriate skill sets, and be factory trained and certified, for each of the airports. The Contractor is responsible for ensuring that such individuals are trained, knowledgeable, and familiar with the facilities and the facilities' procedures. Further, the Contractor shall ensure that such staff shall have appropriate familiarity with badging, safety training and system configuration. The Contractor shall ensure that the staff supporting each airport facility shall be of sufficient numbers so that the unavailability of any one individual shall not deprive the Authority of any of the appropriate skill sets, training, knowledge and areas of familiarization when needed and required.

vi) The Contractor shall be required to conform to the Authority's on-site reporting procedures at each airport facility regarding technician arrival and departure for normal and off hours work. The individual airport reporting procedures will be provided to the Contractor after contract signing.

vii) Preventive Maintenance – Technician Level

Any individual providing Technician Level Maintenance Services as part of this agreement shall be a Contractor factory trained and certified technician.

Preventive Maintenance shall be scheduled to the greatest extent possible during non-peak periods. The Contractor shall consult with the Port Authority to determine periods of peak activity for the various devices.

Scheduled maintenance services shall follow this general procedure:

(1) Preparation – This includes reading and becoming familiar with all manuals and material concerning the equipment, ensuring safety precautions are taken, obtaining all tools, taking the equipment out of service, initiating service documentation, and updating any relevant maintenance tracking programs.

(2) Visually Inspect – Includes checking for loose wires, missing hardware, structural damage, bent pins, damaged cables, cracked displays, peeling labels, rust, etc.

(3) Service and Repair – This includes performing the service and repairing items noted faulty during the inspection.
(4) Test – This includes testing the equipment to ensure functionality in accordance with the Contract.
(5) Return to Service – Once testing is complete and successful the technician shall return the equipment back into service.
(6) Complete Service Documentation – The technician shall complete the service documentation, file paperwork for historical purposes, and update all relevant maintenance tracking information.

As part of the Preventive Maintenance procedures for each piece of equipment, the Contractor shall initial and document the date and time the Preventive Maintenance was performed on a handheld or laptop computer and update a maintenance log stored on the server. The Port Authority may, at any time, access the maintenance log to compare the entries to the scheduled and logged maintenance services within the Maintenance Log and monthly reports provided to the Port Authority by the Contractor and the PA's contracted Airport Parking Operator.

The Contractor shall be responsible for providing all labor, tools and test equipment and any specialized tools required to perform the tasks of the maintenance portion of this agreement as well as all transportation, such as a vehicle, required to transport the technician(s) and store required tools and spare parts.

All consumable office supplies for use by Contractor in its local office shall be the responsibility of the Contractor.

c) Remedial Maintenance—Existing PARCS

i) Remedial Services shall be performed in response to specific events, and shall return equipment to an operating state following a malfunction. Remedial services shall include inspections and necessary diagnostics and tests to determine the causes of PARCS hardware malfunction or failure. The remedial services shall also include the furnishing and installation of components and/or parts that are required to repair malfunctioning system elements.

The Contractor shall perform Remedial Services in response to notifications by the Port Authority under normal conditions as described herein. In addition, the Contractor shall perform Remedial Services in response to notifications by the Port Authority under unusual conditions. Unusual conditions may include a vehicle striking lane equipment thereby damaging the equipment so that the equipment may stop working. Services performed under unusual conditions shall be invoiced to the Port Authority and will be reimbursed under the Extra Work provision of the Contract. The Contractor shall propose hourly rates based on the time of day, day of

week, category of staff, etc. that the services are performed in accordance with the Extra Work provision. On-site maintenance staff can be used for repairs without extra labor charges should they be qualified for the needed repairs. Parts required to perform Remedial Services under unusual conditions, that are not included in the spare parts inventory, shall be invoiced to the Port Authority at the agreed upon rates used to replenish the spare parts inventory under normal conditions and will be reimbursed under the Extra Work provision of the Contract.

ii) Due to the gravity of an equipment malfunction/failure, remedial responses and associated corrective actions shall be provided within the response times specified below. When Remedial Services are required, as determined by the Port Authority, the Port Authority shall notify the Contractor at any time, twenty-four (24) hours per day, seven (7) days per week, three hundred sixty-five (365) days per year. As with Preventive Maintenance, remedial services shall be tracked in the Maintenance Log. The Contractor shall follow Port Authority provided procedures on whom to contact to inform and/or update the status or resolution of a problem.

iii) The Port Authority reserves the right to modify notification policies and procedures at any time throughout the life of the Contract.

iv) Remedial Maintenance of the Existing PARCS at EWR, JFK and LGA shall consist of service calls from operations personnel directly or through a designated call center and/or Port Authority personnel regarding problems with the system not working in accordance with the manufacturer's stated performance, regardless of the cause. The Contractor shall perform remedial maintenance during OPM only if an authorized request for such service is made by the Authority.

v) The Contractor shall be required to respond to all requests for service during the OPM within two (2) hours of notification. If dispatching a technician to provide this service, the technician must report to the requesting facility in accordance with the facility's reporting procedure within the two-hour period after notification. After-hour and weekend support requests to the Contractor shall be made via a phone number that is staffed continuously. The Contractor shall maintain a log of all such calls, which shall include the date and time of the call, the date and time of arrival, description of the problem and the date and time the problem is resolved. Such log shall be submitted to the Facility monthly or upon request of the PA.

vi) The Port Authority Technology Department, or its designee, is responsible for all communications fiber. The Contractor shall, therefore, be required to coordinate activities with the Technology Department for problem resolution. Where a problem has been identified with the system optical fiber, the Contractor shall be responsible for notifying the Technology Department via a phone call to the help desk and email to the network operations group for corrective maintenance, and shall work with the Technology Department until problem resolution is achieved.

However, the Contractor shall be required to assume the responsibility for problem isolation, identification, documentation and correction of problems with peripheral field devices and with the system optical fiber transmission equipment where the Contractor's personnel in the course of carrying out their duties, cause damage to the peripheral or system optical fiber transmission equipment.

vii) Upon request, the Contractor shall be required to perform analysis and diagnosis of problems and other issues with PARCS software. On an "as needed" basis, the Contractor shall be required to provide the Authority with technical support and respond to questions with respect to any equipment and software system. Such support shall be provided during PPM at no additional charge to the Authority.

viii) The Contractor shall be required to comply with Authority procedures for approved work order processing for any work not covered by the lump sum preventative maintenance payment and shall be reimbursed for under the Extra Work, Work Order or Net Costs provisions of the Contract. Work order processing procedures shall be provided to the Contractor after contract execution.

d) Preventative Maintenance—New PARCS

i) The maintenance services to be provided by the Contractor include maintenance for the New PARCS hardware and software components used for airport parking operations, and the subsystems. These include all functionalities and systems referred to in Attachment E, Functional Specifications. The services proposed by the Contractor shall also cover any additional subsystems that are installed by the Contractor as part of this project.

ii) The Contractor shall be required to provide resident technicians at EWR, LGA and JFK during the PPM to maintain the New PARCS after the first lane has been accepted and is in revenue use.

iii) As part of the response to this RFP, the Contractor will propose a preventative maintenance schedule for SWF that does not require resident technicians to report daily to SWF.

iv) As part of the response to this RFP, the Contractor will submit the details of the necessary Preventive Maintenance Tasks for the new PARCS. Scheduled preventive maintenance shall include, but not be limited to, inspection, testing, cleaning, lubricating, painting, adjustment, repairs, the replacement of field installable parts, including external cabinets, that are approaching unserviceable status, and all actions necessary to prevent system failures and extend the PARCS useful life. Contractor shall conduct Preventative Maintenance as accepted by the Port Authority in this Contract.

v) The Contractor will be required to conform to the Authority's on-site reporting procedures at each airport facility regarding technician arrival and departure for normal and off hours work. The individual airport reporting procedures will be provided to the Contractor after contract execution.

e) Remedial Maintenance—New PARCS

i) Remedial Maintenance of the New PARCS at EWR, JFK, LGA and SWF shall consist of service calls from operations personnel and/or Port Authority personnel regarding components of the system not working as designed, regardless of the cause.

ii) The Port Authority Technology Department, or its designee, is responsible for all communications fiber. The Contractor will, therefore, be required to coordinate activities with the Technology Department for problem resolution. Where a problem has been identified with the system optical fiber, the Contractor will be responsible for notifying the Technology Department for corrective maintenance, and will be required to continue work with that group until problem resolution is achieved. However, the Contractor will be required to assume the responsibility for problem isolation, identification, documentation and correction of problems with peripheral field devices and with the system optical fiber transmission equipment where the Contractor's personnel in the course of carrying out their duties, cause damage to the peripheral or system optical fiber transmission equipment.

iii) Upon request, the Contractor will be required to perform analysis and diagnosis of problems and other issues with all PARCS software. In the course of discharging this responsibility, the Contractor shall engage the assistance of the manufacturer to resolve issues related to software problems when necessary and where appropriate. On an "as needed" basis, the Contractor will be required to provide the Authority with technical support and respond to questions with respect to any equipment and software system. Such support will be provided during PPM at no additional charge to the Authority.

iv) The Contractor will be required to comply with Authority procedures for approved work order processing for any work not covered by the lump sum payment and will be reimbursed for under the Work Order, Extra Work or Net Cost provisions of the Contract. Work order processing procedures will be provided to the Contractor after contract execution.

f) System Updates—Existing PARCS

i) The Contractor shall not be responsible for updates to the existing 3M application other than to assist with emergency repairs.

ii) The Contractor shall be responsible for identifying problems with the Existing PARCS and reporting such to the PA. The Contractor will be responsible for identifying any critical system updates issued by third party vendors. The PA will determine if such updates are essential and who would be tasked with installing them. Updates

related to operating system security on workstations are performed by the PA Technology Department. Should the PA determine that an update must be installed which is not under the aegis of TD, through the Work Order process, as outlined in Attachment C, the Contractor will provide a proposal with labor pricing based on the current contract for implementation if so requested by the PA.

g) System Updates—New PARCS

i) System updates shall consist of all actions necessary to incorporate hardware and software updates in the Parking Access and Revenue Control System to ensure performance to original Specifications. Maintaining the System to keep it up to update shall be included in software license costs. Contractor shall provide error correction, updates and third party software only after obtaining the written approval of the Authority. Vendor supplied documentation of updates to reflect these software changes shall be submitted within fourteen (14) days of completion of said software updates. Contractor shall also make new releases of third party software available to the Authority at the Authority's option and expense. The Contractor will not include labor charges for personnel assigned to the airport unless such work is completed during the OPM. The Port Authority's Technology Department will perform updates on all software provided by it for this system. Coordination on testing with the Technology Department is required.

ii) The Contractor shall provide System Updates services on a basis that ensures that the system software, including all third party software, shall be the manufacturer's "current" version. The Contractor shall have fourteen (14) calendar days from the time an update or patch is released by the software manufacturer to process updates and patches in accordance with the requirements stated in the Software Maintenance section herein, except security vulnerability patches, which must be processed as soon as possible.

iii) The Port Authority shall have the option of implementing all PARCS software patches and updates. Fourteen (14) calendar days prior to all PARCS software modifications, patches, updates and upgrades, the Contractor shall provide a Change Control document for review and acceptance to the Authority, containing accurate and complete documentation that describes:
   (1) Patch/update release designation
   (2) Proposed date and time of implementation
   (3) Detailed description of what the patch/update accomplishes
   (4) Full recovery procedures that return the system to its pre-patch update conditions
   (5) List of other installations where the patch has been previously installed, and contact information for those customers if applicable.

iv) Contractor shall coordinate the testing and implementation of all patches and updates with the Port Authority.

v) Contractor shall test all software upgrades, modifications, and changes in the Contractor provided test system prior to implementation in the production system. The Port Authority shall provide approval to migrate to a production environment prior to implementation. Depending on the severity of the upgrade, modification or change, the Authority may choose to witness testing before approving implementation in the production environment.
vi) Contractor shall provide a change control methodology to document system changes and approvals prior to implementation.
vii) The Contractor shall support upgrades to its application based on operating system patch and upgrade requirements (For example, if the PARCS runs on a Microsoft operating system, the software shall be patched according to the Microsoft patch and upgrade schedule without breaking any application. If Microsoft decommissions a specific version of an operating system, the Contractor shall release code compatible with next operating system upgrade prior to Microsoft ending support for current operating system, at no cost to the Port Authority.)
viii) The Contractor shall commit to provide corrective patches and upgrades in the event security vulnerability or system availability issues are found within fifteen (15) business days of said discovery or sooner if approved by the PA.
ix) Copies of all software (and software updates/upgrades made during and after the warranty period) must be provided to the Port Authority at the conclusion of the warranty period.) and put in escrow.

h) Software Maintenance

For all Systems (including their component equipment) covered under this Contract, the Contractor shall provide software maintenance for the operating system, applications software, third party software and third party tools, and database that was furnished and installed by the Contractor. Software maintenance shall include but not be limited to the following:

i) Error Correction
In the event that the System does not meet the operational availability or function in accordance with the manufacturer's stated functionality and performance due to errors in software or any modifications thereto, the Contractor shall correct any such error in the System as identified by the Authority. Errors shall include, but not be limited to, flaws in operations and errors due to flaws in the design and coding of the System.

Upon notification of the error by the Authority or discovery of the error by the Contractor, the Contractor shall dispatch Trained Personnel to repair, replace and correct all malfunctions required for the System to perform in accordance with the manufacturer's stated functionality and meet the operational availability within ten (10) business days from the date of notification. The Contractor shall provide documentation in machine-readable format, if any, relating to the error correction. The corrected software shall be tested by the Contractor in an off-line test

environment. The Contractor shall then prepare a test and demonstrate to the Authority's satisfaction that the error has been corrected and submit it to the Authority for review and approval before the corrected software is installed into the production System. Such corrections to the software shall be provided at no additional cost to the Authority. The Contractor's obligations for the performance and completion of such error correction in order to ensure that the equipment meets the operational availability and functions in accordance with the manufacturer's stated functionality and performance within the time provided for in the above are of the essence of this Contract. The Contractor guarantees that it will use best efforts to complete the performance of such error correction within the time set forth. See below for Service Level Agreements and the associated Liquidated Damages.

ii) Software Updates

The Contractor shall notify the Authority whenever Contractor furnished upgrades and/or enhancements to operating system, the application software, third party software or third party software tools used by the System when they become available. The Contractor shall also provide the Authority with an analysis of the potential effects of such upgrades/enhancements on the System. This analysis shall include, at a minimum, the following:

(1) Compatibility of the application software with the new operating system or third-party software;
(2) Compatibility of the upgrade with the system architecture, server and communications infrastructure ;
(3) Infrastructure improvements required to support the upgrade;
(4) Potential increases or decreases in equipment performance;
(5) The availability of product support for the current (older) version of the operating system or third party software;
(6) The cost of the software upgrade, including testing and any other tasks which may be associated with the upgrade.

The Authority will then determine whether or not to order the upgrade. If the Authority selects the upgrade, the Contractor shall perform the upgrade on the System, test the system, and update the documentation, all in accordance with the sections testing and documentation. The Contractor will be compensated for this Work under the net cost provisions of the Contract (Compensation for Net Cost Work). Any updates to system shall be put in escrow.

iii) Adaptive Changes

In the event changes to the computing or network environment are disruptive to the System or prevent the System from meeting the operational availability or function in accordance with the manufacturer's stated functionality and performance, the Contractor shall implement corrections to the software or System configuration to

mitigate those changes to the computing environment. Upon notification of the disruption by the Authority or discovery by the Contractor that the System is not operating in accordance with the manufacturer's stated functionality and performance, the Contractor shall dispatch Trained Personnel to correct the disruption and restore System operation. The Contractor guarantees that it will use its best efforts to implement required corrections as soon as practical, based on the nature of the disruption and criticality of the lost services. The Contractor shall implement all changes, test the System, and update the documentation. The Contractor will be compensated for this Work under the net cost provisions of the Contract (Compensation for Net Cost Work).

iv) Monitoring Application to Maintain System Performance

The Contractor shall be responsible for routine operation of all software and data used by the application, application files, diagnosing and effecting correction of all problems that impact operation of the applications software and its data, including, but not limited to, the tasks listed herein.

The Contractor shall employ system monitoring devices and programs, and diagnostic tools to ensure that all aspects of the application software are operating properly and the System is meeting all specified performance criteria. This work shall include, but not be limited to the following:

(1) monitor disk usage to verify adequate empty disk space available for program usage and data files (i.e., temporary files, logs, etc.,)
(2) monitor logs to verify log files are saved to removable media and log files are purged on a regular basis and purge log files that exceed the data retention period
(3) monitor the database to verify database operation and ensure its performance is within acceptable tolerances and implement corrections to maintain acceptable performance,
(4) monitor the application software, to ensure its performance is within acceptable tolerances and meets the operational availability requirements

For the existing PARCS, based on these reviews, the Contractor shall perform required activities and take corrective actions (e.g. de-fragmenting disk files, purging obsolete files from directories, perform database maintenance, etc.) to ensure its performance is within acceptable tolerances and meets the operational availability requirements.

With regard to the New PARCS, the Contractor shall provide the PA with a detailed plan on how to perform the suggested activities.

v) Manage Cyber Security Vulnerabilities

The Contractor shall monitor, evaluate, track, log, and immediately report on all cyber-security vulnerabilities or other vulnerabilities related to the software used in the equipment. The Contractor shall work with the Authority to address any identified vulnerabilities and mitigate all security/malware/virus alerts in accordance with the procedures identified The Port Authority's Guide for System Administration which will be given to the Contractor upon commencement of the Contract.

vi) Testing

Prior to implementing any changes on the production system, the Contractor shall test the System in a separate development/test system environment to ensure that the changes are compatible with the application and other installed components. Testing shall follow the prescribed order of events listed below and include, but not be limited to, the following Contractor activities:

(1) Provide an acceptance test plan and procedures for Authority approval,
(2) Install all changes on a separate stand alone off-line test environment,
(3) Conduct Contractor pretests, and once testing confirms that the changes are compatible with the application and environment, then conduct Authority-witnessed testing and submit a test report. Once the test report is approved by the Authority, the Contractor shall make arrangements with the Manager to schedule the changes to the production environment.
(4) Complete the Authority's approved change management request form and obtain approval from the Manager before implementing the changes in the production environment.
(5) Install the changes to the production environment and confirm with the Authority that the System operation is restored.

vii) Documentation

The Contractor shall provide documentation in support of all changes to the System environment, including a description of changes, a list of updated hardware/software components, and a list of all System components that are impacted by the changes as well as a specific timetable/schedule for making and implementing changes. The Contractor shall update the system documentation in machine-readable format to for any and all work related to all changes to the System and/or the System environment, to reflect as-built conditions. The documentation shall include but not be limited to all drawings, design documents, software and hardware manuals/documentation, user manuals, help desk and troubleshooting guides, etc.

The Contractor shall track all changes, not only to the source code, but also to all other components of the System. This includes, but is not limited to, configuration files, scripts, database configuration files, where applicable third party applications, and any other affected files. The Contractor shall update any affected

documentation and deliver updates on a quarterly basis. The Contractor shall coordinate its work with the Technology Department and it is the Contractor's responsibility to maintain the documentation for all firewall rules used to configure the network and ensure that the documentation is up-to-date. All system documentation, and any updates to system documentation, shall be placed in escrow.

i) Maintenance Staff
   i) The Contractor shall provide resumes for the proposed maintenance staff as a part of the Proposal. The PA must be advised of any changes to the staff indicated at the proposal stage and accepted as part of this agreement.
   ii) The Contractor shall provide detailed job descriptions for all positions as a part of the Proposal
   iii) The Contractor shall adhere to the requirements noted in (D) below, and then propose an appropriately sized staff to ensure successful performance of routine Preventive Maintenance and Remedial Services Maintenance. The Contractor's staffing plan shall take into consideration extenuating circumstances such as illness, family emergencies, vacations, etc. such that at all times the required number of technicians are available. Anticipated on-site hours and typical numbers of technicians on-site at any one time shall be provided by the Contractor in their proposal.
   iv) The Contractor's maintenance staff that will perform the scope of work described shall consist of:
      (1) Factory trained hardware technicians available throughout the life of the maintenance Contract to handle Preventive Maintenance.
      (2) Factory trained hardware technicians to handle remedial maintenance services calls, available by text, email, fax, phone, or pager twenty-four (24) hours a day, seven (7) days a week, three hundred sixty-five (365) days a year.
   v) Port Authority shall have the right to have any personnel removed from the Contract at its sole discretion. Contractor shall immediately remove personnel from Port Authority work sites upon notification and replace them with qualified staff that have been approved by the Authority.

j) Electronic System Maintenance Tracking System
   i) The Contractor shall utilize a Maintenance Tracking System, provided by the Contractor, to monitor and record all scheduled, requested, and performed maintenance services. Contractor shall propose the Maintenance Tracking System to the Port Authority for review and approval prior to the implementation of such system
   ii) The Contractor shall fill in all required fields, completely, for all Preventive Maintenance and Remedial Maintenance Services scheduled and performed at the Port Authority.

iii) The Contractor shall submit Monthly Maintenance Reports in the Port Authority-approved format to designated personnel during the Contract period. All reporting requirements shall be determined at the time of Contract start.

9) Warranty Service Period Requirements

The PARCS warranty period at each airport shall last at least twelve (12) months and shall commence when the Operational Acceptance Test has been successfully completed for that airport and the Contractor has received written notice of formal system acceptance from the Port Authority for the airport. The Contractor shall provide preventative and remedial maintenance on all systems that are operating prior to starting the warranty period at no cost to the Port Authority.

The Port Authority requires all new work to be warranted against defects in material and workmanship for a period of at least twelve (12) months. Contractor shall provide details concerning its warranty coverage in its proposal. During the Product Warranty Period, commencing with the acceptance date of the Operations Acceptance Test at each facility, the Contractor shall provide Warranty Service on all equipment and software furnished under the Contract such that the System will perform in accordance with the Contract, twenty-four (24) hours a day, seven (7) days a week, including Holidays. Such performance of the PARCS shall be referred to as performing in “Working Order”. All-inclusive costs (parts, labor, maintenance, warranty repairs, Contractor travel time, Contractor expenses, etc.) incurred during the warranty period shall be provided without additional cost to the Port Authority.

Contractor shall provide an updated preventive maintenance schedule within thirty (30) days of successful completion of the Operational Acceptance Test. This will be based on the preventative maintenance schedule that will be provided at the time of proposal. The preventative maintenance schedule shall be updated monthly and provided to the Authority for review and comment.

The Contractor guarantees and warrants that work done and items procured shall (a) meet the requirements of the Contract and (b) be free from defects in design, materials and workmanship. This guarantee and warranty shall apply to all discrepancies and defects that are discovered within twelve months the Operational Acceptance Test completion. The terms of Warranty for the defective items shall be extended for any periods that work done or equipment installed cannot be used for the purpose intended because of the discrepancy or defect.

The Warranty Period of the PARCS shall include all preventive and corrective maintenance, including repair of vandalized equipment, except that the cost of parts used to replace vandalized parts other than wear-related items shall be borne by the Authority.

Excluded from the warranty are damages due to Acts of God. For services that are excluded from the warranty, the Contractor shall use the rates as agreed upon in the maintenance section of the Contract for the relevant equipment. On-site maintenance staff must be used for repairs without extra labor charges.

Contractor is solely responsible for all costs of parts and labor incurred during the Warranty Period.

10) DELIVERY AND STORAGE

The Contractor shall be responsible for insuring all shipped items. Any items damaged during shipping shall be replaced and shipped to the Port Authority, by expedited means if requested, at no additional cost to the Port Authority.

The Port Authority shall provide the Contractor with a designated storage/staging area for PARCS equipment that has not been installed. The Contractor shall describe in its Proposal the total square footage of area required for all of the airports, and what is planned to be stored in the area. The Port Authority shall determine the exact location(s) after Contract Award. The total square footage will be provided by the Port Authority among all four airports, but it is not guaranteed that equipment for a certain airport will be stored at that airport. It is the Contractor's responsibility to protect the equipment from theft and damage until final acceptance including installation of fencing, locks, and any other security provisions. Should the stored equipment be stolen or damaged prior to final acceptance, the Contractor shall replace the equipment at no additional cost to the Port Authority.

After equipment is accepted, costs (time and material) for repair or parts replacement, components, etc., damaged or rendered unserviceable due to apparent and provable misuse, abuse, vandalism or negligence by Port Authority or Port Authority employees or the using public are excluded as a cost incurred by the Contractor. Also excluded from the costs incurred by Contractor are damages due to Acts of God that occur after acceptance.

11) CONSUMABLES

The Contractor shall provide the Port Authority with receipt specifications and parking and valet ticket specifications (front and back sides of a typical parking ticket delineating required formats; magnetic stripe or barcode location; and proposed ticket printer) for the New PARCS within thirty (30) days following Contract Award. The ticket format shall be such that the Port Authority can input its required information on the ticket and submit the revised ticket to the Contractor for review and revisions as required. An agreed upon ticket format for each facility shall be finalized within sixty (60) days after Contract Award. Ticket stock delivery shall occur prior to or concurrent with the first equipment delivery to the Port Authority. Ticket stock, receipt paper, and proximity cards shall be printed with the Port Authority logo and branding.

The Contractor shall provide a twelve-month supply of receipt paper and tickets to the Port Authority upon contract execution. The number of tickets that are supplied shall be based upon the number of parking transactions processed plus a 50% allowance for growth in the number of transactions processed. The Contractor shall submit proofs for each component for review and approval by Port Authority prior to placing any order.

The Port Authority shall not be tied down to any one particular ticket supplier. As such, ticket specifications shall be reproducible by multiple ticket printers.

12) PARCS SYSTEM INSTALLATION

a) Acceptance Testing

Acceptance testing shall serve to verify the functional performance of the PARCS and its components to ensure adherence to these in Attachment E, Functional Specifications. The Acceptance testing process shall not take away from or reduce the responsibility of the Contractor to provide a finished and fully functioning system that meets all requirements of the Functional Specifications. Each application software package, firmware, and hardware equipment component delivered by the Contractor shall undergo acceptance testing as part of the installation process. The acceptance testing of the PARCS shall occur in the following sequence:

i) Factory Acceptance Test (FAT), Section b below;
ii) Field Acceptance Tests, Section c below;
   (1) Lane Acceptance Test (LAT)
   (2) Site Acceptance Test (SAT)
iii) Operational Acceptance Test (OAT), Section d below;
iv) Final System Acceptance (FSA), Section e below

The PARCS shall successfully pass each testing phase before the next testing phase commences. The LATs shall not begin until the FAT has been successfully completed; the SATs shall not begin until all LATs for a given lot at a facility have been successfully completed; and the OAT shall not begin until all Site Acceptance Tests at a facility have been successfully completed. Tests shall not be excluded or conducted out of sequence without prior written authorization from the Port Authority.

Thirty (30) days prior to the anticipated completion of all LATs for a parking facility's implementation, the Contractor shall submit a written request for starting the Site Acceptance Test. A Site Acceptance Test shall be performed for each individual parking facility after all LATs for that parking facility have been successfully completed. Following successful completion of all Site Acceptance Tests, an OAT shall be conducted to assess the entire PARCS installation as a system.

The Contractor shall submit the proposed Phasing Plan as outlined in the submittal guidelines, which are found in the Information for Proposers at the beginning of this document. Testing shall not disrupt the normal entering and exiting of vehicles from the

parking facility areas regardless of whether the lane is connected to the Existing PARCS or the New PARCS.

b) Pre-Acceptance Testing

During the development phase, prior to the Factory Acceptance Test, the Contractor shall test the software and hardware components individually and as an integrated system to ensure that they perform according to the Contract. While this testing is primarily conducted by the Contractor without regular monitoring by the Authority, the Authority shall have the right to review the Contractor testing and test progress at any time. Test milestones for pre-acceptance testing shall be reflected in the Project Plan and Schedule, and testing progress shall be documented in the Contractor's regularly issued project status reports.

c) Acceptance Testing Provisions

The Contractor shall prepare and deliver to the Authority a comprehensive Acceptance Test Plan that describes all the activities and tasks associated with testing during each test phase. At a minimum, the Contractor's Acceptance Test Plan shall contain the following elements:

i) A summary statement of the purpose and goal of each test phase, the method of testing, a description of the overall test environment, test equipment details, test equipment configuration sketches and diagrams, including cabling requirements, and a specification of the hardware and software required for the test: including the number and type of devices to be used during the test or the method of simulation.
ii) A testing plan identifying each individual test to be performed, the anticipated duration, staffing requirements, the purpose of the test, the conditions that shall exist at the start of the test and the conditions/results expected to exist at the conclusion of the test.
iii) Detailed test procedures that identify each step to be performed, how the step will be performed and the anticipated results of each step.
iv) A description of the outputs (reports, database listings, statistical analyses, etc.) to be provided to the Authority to document the test results.
v) Test incident report forms and test incident log.

After receipt of each Acceptance Test Plan, the Authority will formally comment on its content, and if necessary, the Contractor shall make appropriate changes to the Acceptance Test Plan and resubmit it for Authority review and approval. The Authority may request subsequent changes to the Acceptance Test Plan in the event of modifications or additional functionality to the system hardware or software.

The Authority may, at its discretion, observe a portion of, or all of each acceptance test, as it deems necessary.

When all tests for a testing phase have been executed to the satisfaction of the Authority, the Contractor shall prepare and deliver to the Authority an Acceptance Test Report along with the Contractor's written certification that the system component has successfully passed all tests for that specific test phase. The Acceptance Test Report shall contain at a minimum the following sections:

i) Summary of the test phase.
ii) Description of the tests performed to include: Test conditions at start and end of each test, expected test results with Pass/Fail criteria, and actual test results.
iii) List of punch list items that need to be completed and retested.
iv) Action plan to conduct the next iteration of the test phase or a statement that the phase was completed successfully.

The Authority shall evaluate each Acceptance Test Report and notify the Contractor of its evaluation. No acceptance test phase shall be initiated without the Authority's written approval of the Acceptance Test Plan specific to that phase, and no test phase shall be considered complete, nor may the Contractor proceed to the next step of the project until the Authority has approved, in writing, the Contractor's Acceptance Test Report for the previous phase.

b) Factory Acceptance Test (FAT)

Within ninety (90) days after Contract signing, the Contractor shall submit a Factory Acceptance Test Plan to the Authority for review and approval.

Following written approval of the FAT Plan by the Port Authority, the Contractor shall conduct the FAT according to the following requirements:

i) A FAT shall be conducted to verify the functional performance of all systems, subsystems, and components of the PARCS to ensure adherence to these Functional Specifications, prior to installing any equipment at the Port Authority.
ii) To verify that all the functionalities described within these Functional Specifications are achieved, the Contractor shall demonstrate the performance of the PARCS at a location mutually agreed upon by the Port Authority and the Contractor. Generally, the FAT takes place at the Contractor's manufacturing facility or central distribution center. As part of the FAT, the Contractor shall configure a lane of each type with all applicable components, or standalone device if the particular device is not part of an entry/exit lane (e.g. server, workstations, etc.), to simulate the configuration as installed at the Port Authority, including Pay-on-Foot machines. The Contractor shall provide all ancillary items necessary to complete the FAT including setting up a credit card test bed for testing purposes; supply credit cards of all types for testing; provide equipment and test tags for *E-ZPass® Plus™* testing; provide all ticket and ticketless media needed for each transaction type; and provide all keys to access equipment housings.

iii) All systems, subsystems, and components of the PARCS shall successfully complete a FAT prior to the shipment of any equipment to the project site. The Port Authority will provide written acceptance of the FAT. Contractor shall not ship any equipment, subsystem, or component prior to receipt of written acceptance of the FAT by the Port Authority's representative.
iv) In addition to all standalone systems being tested separately, the Contractor shall test the system in its entirety with all subsystems integrated together.
v) Contractor shall design and construct a device for testing the LPR system. This device should be a cart on four wheels with hooks for attaching license plates at an appropriate height (simulating a passenger vehicle) for LPR camera detection. The cart shall be lightweight but have adequate metal to activate an inductive loop thereby simulating a passenger vehicle driving over an inductive loop in the lanes. The cart shall have a handle for ease of manual manipulation by the person testing the lanes.
vi) The Contractor shall notify the Port Authority that it is ready to schedule a Factory Acceptance Test of the System or any individual subsystems.
vii) A pre-acceptance test shall be conducted by the Contractor in advance of the formal acceptance test, using the Inspection and Test procedures approved by the Port Authority's Project Manager to demonstrate that the System is ready for the formal acceptance test that will be witnessed by the Port Authority's Project Manager.
viii) Testing shall be performed by the Contractor and witnessed by the Port Authority's Project Manager using test procedures submitted by the Contractor and approved by the Port Authority. The Port Authority has the right to include not more than five (5) additional Port Authority professionals, who have been deemed the technical and operational experts to assist in witnessing the Factory Acceptance Tests.
ix) Testing shall be conducted with all devices and components integrated as a System with use of simulation expressly limited to perform stress and performance testing. Testing shall demonstrate proper System operation in the fully integrated environment to validate the intended function and performance of all field devices and infrastructure components. Testing shall also demonstrate that all devices and components function in accordance with the Contract requirements and operate as a fully integrated system.
x) The use of simulated inputs and simulated outputs shall only be used in the event that conditions cannot be replicated or to demonstrate requirements for future capabilities or expansion.
xi) The success (pass) or failure of each test and any detailed test results will be recorded by the Port Authority's Project Manager's designated representative.
xii) All hardware, software, network, equipment, external connectivity, licenses and labor required for the test shall be furnished by the Contractor.

The Factory Acceptance Test shall be conducted in its entirety in order to demonstrate that every feature and function of the hardware, software, firmware, and network components of the System are fully integrated and are in conformance with the Contract documents. Testing shall demonstrate end-to-end connectivity and full

functionality of all System components. Testing shall include a stress test to demonstrate that the System meets the performance requirements when processing all devices in the final system configuration. Simulated inputs may be used to demonstrate that the full processing load can be achieved.

The Contractor shall demonstrate that the automatic failover from the primary server(s) to the secondary (backup) server(s) and the complete restoration of the primary server(s) subsequent to the failover operates successfully.

The Contractor shall demonstrate that Users can access all features of and control the System.

In the event of a test failure, the Contractor shall make all repairs or modifications required for passing the test. The failed test shall be repeated until the results are satisfactory to the Port Authority. Any subsequent planned tests that, in the opinion of the Port Authority's Project Manager, are dependent on the satisfactory passing of the failed test shall not be performed until the failed test is repeated and has satisfactorily passed. To demonstrate a satisfactory resolution of a failed test, the Port Authority's Project Manager may require that the Contractor perform additional tests. These additional tests shall be made at the expense of the Contractor, at Port Authority's sole discretion.

If, in the opinion of the Port Authority, there are an excessive number of failed tests, or tests that cannot be performed in a timely manner, the Factory Acceptance Test shall be halted and the Contractor shall repeat all or part of the Test, at the discretion of the Port Authority's Project Manager, at a later date.

Should it be necessary for the Port Authority to attend more than one Factory Acceptance Test session due to Contractor delays, product failure, failure to pass approved testing procedures, inability to complete the test in the scheduled time period or failure to implement approved testing procedures, the Contractor shall bear all costs incurred by the Port Authority for each additional test session where up to three (3) Port Authority representatives may attend. Such costs for Port Authority representatives for each additional Inspection and Test session will be deducted from the Contractor's compensation, at Port Authority's sole discretion.

Prior to the conclusion of the test, the Contractor shall submit to the Port Authority's Project Manager an internationally recognized certification conforming to SSAE16 SOC 2 Type 2, or approved equivalent, that the security policies and practices employed in the System configuration, setup and operation provide the protections stated in the Audit Controls Requirement Contract Checklist (Attachment J), Technology Standards for the Port Authority (Attachment K) and Cyber Security Guidelines (Attachment M).

At the conclusion of the test, the Contractor shall submit to the Port Authority's Project Manager an acceptance test report for the purpose of verifying and validating the accuracy and integrity of the System as installed. The Port Authority's Project Manager will review the report and respond; indicating approval or noting changes required either in the performance of the Work or in the report. The Contractor shall make all changes and perform such necessary Work as the Port Authority's Project Manager may direct, prior to the start of the Operational Acceptance Test.

Neither the witnessing of a test by the Port Authority's Project Manager, or the waiving of a right to witness a test shall relieve the Contractor of the responsibility of furnishing the System that is in compliance with the Contract requirements. The witnessing of any tests by the Port Authority's Project Manager's designated representative, or the approval for shipment of System shall not be deemed as acceptance of the System, the associated control, electronics and communications equipment.

Deviations shall be defined as the following:

(1) Level A deviations – Minor deviations that can be corrected by the Contractor without affecting testing.
(2) Level B deviations – More severe deviations that must be corrected prior to the conclusion of the current test procedures.
(3) Level C deviations – All testing must stop and the current test restarted after the correction of the identified deviation.

The FAT shall be considered successfully completed when all systems, subsystems, and components have passed their respective test procedures and all test documents have been signed by the Port Authority and the Contractor. Minor deviations shall not be considered grounds for failure of the FAT. Major deviations found during the FAT shall result in the retest of the respective equipment, software, or subsystem before the FAT is considered successfully complete. Based on the severity of the deviation, a complete retest may be required.

The Contractor shall provide the Port Authority a plan for the FAT in accordance with the submittal guidelines. Test procedures shall be provided for each lane type or device type and test procedures shall include:

(1) Network diagram that identifies all components used in the FAT and illustrates their connectivity;
(2) narrative describing the general procedures to be followed;
(3) definition of all minor and major deviation types;
(4) checklist of all items necessary to conduct the test (e.g. unpaid tickets, exceptions tickets, credit cards, transponders, equipment keys, license plates, etc.);
(5) checklist for the components of each lane or device;

(6) signature page for all FAT participants' signatures;
(7) step by step instructions for testing each functionality;
(8) tests for verifying reports;
(9) area within each test section to denote "pass" or "fail";
(10) section for listing and describing test deviations; and
(11) section for Authority comments.

Factory Acceptance Tests shall be conducted by the Contractor and observed by the Authority. The Contractor shall perform each test as described in the Factory Acceptance Test Plan in its entirety with the use of actual system equipment and the use of simulated inputs and/or simulated outputs, if necessary. The Contractor shall determine the detailed results of each test and the Authority shall record the success (pass) or failure of each test. Except as approved by the Program Manager, the Factory Acceptance Test shall be conducted at the Contractor's facilities.

The factory test shall involve, at a minimum, the inspection by the Authority of all major physical components of the Parking Access and Revenue Control System as well as the testing of the functionality of the PARCS in a controlled environment in accordance with the Factory Test Plan. The Contractor shall assemble the PARCS, including all major components, at the place of manufacture.

i) Internal Contractor Tests

All equipment shall have successfully passed formal manufacturing tests and quality assurance inspections to validate compliance with the Contract prior to the start of the FAT. Records for formal internal Contractor testing and inspection for performance, materials quality and/or workmanship shall be maintained by the Contractor and made available if so requested by the Port Authority prior to the start of any acceptance test.

Contractor shall have readily available proof of product reliability analysis and testing should reliability become a problem at any time from the beginning of installation testing through the final Operational Acceptance Test period.

Prior to the initiation of testing, the Contractor shall provide draft copies of all documentation required for system operation and conduct training for preparing test participants for testing.

c) Field Acceptance Tests

There are two (2) components of Field Acceptance Testing: Lane Acceptance Testing and Site Acceptance Testing.

Within one hundred twenty (120) days of Contract execution, the Contractor shall submit a Field Acceptance Test Plan to the Authority for review and approval that demonstrates compliance to Contract requirements and proper installation techniques. The Contractor shall conduct a Field Acceptance Test at the Authority's facilities after any equipment is installed in the field. After approval by the Authority of the Contractor's Installation Plan, the Contractor shall deliver the PARCS equipment and components to the Authority's site(s). A field inspection of the PARCS equipment will be made by the Authority, and if any equipment has been damaged or does not comply with the requirements hereof, the Contractor shall be notified in writing, and it shall replace the equipment at its own expense.

After installation and agreement by the Authority to initiate testing, the PARCS shall be tested in compliance with the Field Acceptance Test Plan. The Field Acceptance Test shall be conducted with all devices and components integrated as a system at each of the Authority's sites. The test scripts to be used shall include, but not be limited to, those test scripts used for the Factory Acceptance Test, and any additions as required to encompass all field devices (e.g., local processors, network components, infrastructure, etc.). Any repairs, construction, or modifications as required to comply with this Section shall be performed by the Contractor without additional cost to the Authority. The Contractor shall perform Field Acceptance Tests at the facilities as detailed on the project schedule.

The Contractor shall provide the Authority with a Field Acceptance Test Report at the conclusion of all Lane Acceptance Tests and Site Acceptance Tests. for the purpose of verifying and validating the accuracy and integrity of the Revenue Control System as installed. The Authority will review the report and respond, indicating its approval or noting changes required either in the performance of the work or in the report. The Contractor shall make changes or perform additional work as the Authority may direct prior to the start of the Operational Acceptance Test.

i) Lane Acceptance Tests (LATs)

LATs shall be conducted by the Contractor to demonstrate to the Port Authority that the equipment was not damaged during shipping, was installed properly as per the Contractor's shop drawings, functions in accordance with the Contract requirements and other Authority approved documentation, such as user manuals and is connected to the application servers via the network.

After successful completion of the FAT the equipment, software, and subsystems may be installed at the Port Authority, based on a Port Authority-approved schedule. When a lane installation has been completed, the Contractor shall conduct its internal testing of the installed equipment. Internal testing shall follow the identical LAT test procedures that were approved by the Authority.

Upon successful completion of the Contractor's test, the Contractor shall perform the LAT to verify performance. The Port Authority shall observe the LAT. The LAT shall only be observed by the Port Authority after a fully completed and signed test script verifying successful completion of the Contractor's internal testing is submitted. Signed internal test scripts shall be submitted at least five business days prior to the scheduled test with the Port Authority.

LATs shall be conducted at the Port Authority facilities for each entry lane, exit lane, bus lane, POF, and PSCS detector. The Contractor shall not activate any entry/exit lane for service until its LAT has been successfully completed, and the Port Authority has notified the Contractor that it is ready to put the equipment in operation.

The Contractor shall provide test procedure documents for LATs in accordance to the submittal guidelines. LAT Test Procedures Documents shall be provided for each lane type or device type and test procedures shall include the following sections:

(1) Narrative describing the general procedures to be followed;
(2) Definition of all minor and major deviation types;
(3) Checklist of all items necessary to conduct the test (e.g. unpaid tickets, exceptions tickets, credit cards, transponders, equipment keys, etc.);
(4) Checklist for the components of each lane or device;
(5) Signature page for all LAT participants' signatures;
(6) Detailed step by step instructions for testing each functionality;
(7) Tests for all patron processing procedures including valid normally accepted patron activities such as normal entry and exit and unacceptable patron activities such as backing out of entry and exit lanes, pulling a ticket and backing out, etc.;
(8) Tests to ensure that the proper rate structures are being used;
(9) Tests for verifying the reporting requirements;
(10) Area within each test section to denote "pass" or "fail"; and
(11) Section for listing and describing test deviations.

The Contractor shall provide, at a minimum, all ancillary items necessary to complete the LATs for testing purposes; supply and operate vehicles for testing; supply licenses plates covering all of the states specified as part of LPR processing requirements stated herein; supply credit cards of all types for testing; provide *E-ZPass®* and AVI transponders; provide all ticket and ticketless media needed for each transaction type; and provide all keys to access equipment housings. In addition, the Contractor shall make available sufficient personnel to perform the LAT in an efficient and timely manner.

The LAT shall be considered successfully completed when all components have passed their respective test procedures and all test documents have been signed by the Port Authority and Contractor. The Contractor shall agree to credit the Port Authority from its total contract value for any travel and/or labor costs incurred by

the Port Authority as a result of retesting a failed lane. Back office reports for individual lanes shall be checked for completeness, accuracy, and availability by the Authority or its representatives.

ii) Site Acceptance Tests (SATs)

The Site Acceptance Tests shall test each parking facility's equipment installation as a system, e.g., all entry lanes, exit lanes, POFs, communication to the workstations, PSCS, and Servers. The test shall include all aspects of PARCS software functionality applicable to the facility, e.g. customer loyalty programs, mobile payment, reporting, etc. The Site Acceptance Test is a pass/fail test that relies upon the operation and status of equipment and system reports of an individual facility. The Port Authority and the Contractor shall collectively select an "initial start-up date" for each Site Acceptance Test. Site Acceptance Tests shall run for seven (7) days beginning at the initial start-up date and continuing for seven (7) consecutive 24-hour periods with no major deviations. Site Acceptance Tests shall be performed for each individual parking facility only after all equipment has been installed and all LATs in a parking facility have been successfully completed and approved.

During a Site Acceptance Test only routine maintenance procedures, as defined by the preventive maintenance manual and according to industry standards, shall be permitted. All other maintenance procedures shall be approved in writing by the Port Authority before they are performed; otherwise, they shall constitute a failure of the Site Acceptance Test and a mandatory restart.

The Port Authority reserves the right to be present for all maintenance services during the Site Acceptance Tests.

The Contractor shall submit a Site Acceptance Test Procedures Document in accordance with the proposal submittal requirements. Site Acceptance Test Procedures Documents are intended to outline procedures for monitoring the overall performance of the PARCS and shall not include test procedures for individual lanes or components. The Site Acceptance Test Procedures Document shall include:

(1) Narrative describing the general procedures to be followed;
(2) Methodology for calculation of downtime for the various PARCS components; and
(3) Electronic tracking document to be used during the Site Acceptance Test period for documenting failures and downtime.

The performance criteria for successful completion of the Site Acceptance Test shall include:

(1) All subsystems shall be operationally available 100% of the time during the seven (7) day test period.
(2) If any single component fails, the seven-day SAT shall halt and start over upon the replacement or correction of the problem. If, in the opinion of the Authority, the number of failures are excessive, the SAT shall start over from the beginning and be conducted over the full seven (7) days.
(3) In addition to the comprehensive reports generated during the Site Acceptance Tests, the Contractor shall provide to the Port Authority a one (1) page summary report that clearly provides the overall percentage of system downtime, causes of that down time, and any incidental cost incurred during each test.
(4) The Contractor shall provide to the Port Authority a corrective action report that provides a detailed description of each failure that occurs during each Site Acceptance Test. The corrective action report shall include the type of failure, why the failure occurred, what was done to remedy the failure, and whether or not the failure resulted in a restart of the Site Acceptance Test.
(5) All reports shall be 100% accurate and be reconcilable against each other for the seven (7) day testing period otherwise the test shall be deemed a failure, problems shall be corrected, and the test shall be restarted from the beginning.

d) Operational Acceptance Test

Two (2) months prior to conducting Operational Acceptance Testing at each airport, the Contractor shall submit an Operational Acceptance Test (OAT) Plan, unique to the airport to be tested, to the Authority for review and approval.

Following written approval of the OAT Plan by the Port Authority, the Contractor shall conduct a separate OAT for each airport.

The OAT shall be comprised of all equipment, systems, and subsystems performing under actual conditions, e.g., patron use, normal activity recording, and reporting procedures. This OAT shall demonstrate, over a period of thirty (30) consecutive calendar days, the successful performance of all aspects of the PARCS.

During the OAT only routine maintenance procedures, as defined by the preventive maintenance manual and according to industry standards, shall be permitted. All other maintenance procedures shall be approved in writing by the Port Authority before they are performed; otherwise, they shall constitute a failure of the OAT and a mandatory restart.

The Port Authority reserves the right to be present for all maintenance services during the OAT.

For purposes of the OAT, a subsystem is defined to be any one of the following:
(a) Application servers

(b) Data servers
(c) Credit card authorization and settlement system
(d) Data communication system
(e) PARCS workstations
(f) Entry lane
(g) Exit lane
(h) POF
(i) PSCS
(j) LPR system
(k) LPI system
(l) AVI system
(m) Loyalty programs
(n) Barcode readers
(o) Signs
(p) Proximity card access system
(q) Intercom System
(r) *E-ZPass® Plus™* System
(s) In booth Camera system
(t) All other systems specified in Attachment E, Functional Specifications

The OAT shall begin after all facilities, parking lots, POF, etc., have successfully completed their respective Site Acceptance Tests on a date mutually selected and agreed to in writing by the Port Authority and the Contractor at a time designated by the Port Authority. The OAT monitors system performance of the entire system operating as a single unit. The Contractor shall submit an OAT Test Procedures Document in accordance with the submittal requirements. OAT Test Procedures Documents are intended to outline procedures for monitoring the overall performance of the PARCS and shall not include test procedures for individual lanes or components. The OAT Test Procedures Document shall include:

(a) Narrative describing the general procedures to be followed;
(b) Methodology for calculation of downtime for the various PARCS components; and
(c) Electronic tracking document to be used during the OAT period for documenting failures and downtime.

The OAT shall continue for thirty (30) consecutive twenty-four (24) hour periods during which all the performance criteria, stated below, shall have been met. If during the thirty (30) day period the system fails to meet any one of the following specified performance criteria, the test shall begin anew on a day agreed upon by the Port Authority and the Contractor. The Contractor shall agree to credit the Port Authority from its total contract value for any travel and/or labor costs incurred by the Port Authority as a result of retesting the system.

The performance criteria for successful completion of the OAT shall include:

(a) No individual subsystem shall be operationally unavailable for four (4) or more hours cumulative during the thirty (30) day test period.
(b) No individual subsystem shall be operationally unavailable for more than two (2) consecutive hours.
(c) If any single component fails more than once during the thirty (30) day period for the same reason, it shall be replaced upon the second failure with a newly manufactured component of the same type and the test shall continue.
(d) No component of a given type (e.g., cashier station, exit station, barrier gate, entry station, etc.) shall fail more than three (3) times during the thirty (30) day test period for the same reason. Upon the fourth failure all components of that type shall be replaced to correct the common deficiency, and the test shall be restarted from the beginning.
(e) In addition to the comprehensive reports generated during the OAT, the Contractor shall provide to the Port Authority a one (1) page summary report that clearly provides the overall percentage of system downtime and causes of that downtime.
(f) The Contractor shall provide to the Port Authority a corrective action report that provides a detailed description of each failure that occurs during the OAT. The corrective action report shall include the type of failure, why the failure occurred, what was done to remedy the failure, and whether or not the failure resulted in a restart of the OAT.
(g) All reports shall be one hundred (100%) percent accurate and can be reconciled against one another over the thirty (30) day testing period, otherwise the test shall be deemed a failure, problems shall be corrected and the test restarted.

A subsystem shall be considered unavailable as long as any major component of the subsystem is not functioning properly. As an example, the major components of an entry lane include but are not limited to:

(a) Lane Open/Closed Signs
(b) Vehicle detector devices
(c) Intercom
(d) Pinhole camera
(e) Barrier gate
(f) Entry Station
(g) PSCS devices – sensors and signs
(h) AVI reader
(i) Proximity Card Reader
(j) LPR Camera and video analytics equipment
(k) Data communication

(l) Power supply
(m) UPS
(n) *E-ZPass® Plus™*

An inoperative subsystem shall not be deemed unavailable if it has become inoperative because of:

(a) Outage of line power beyond required duration of UPS power backup;
(b) Malicious damage or vandalism to a component(s) by employees, patrons or others;
(c) Network connectivity issues beyond the PARCS;
(d) PARCS failures due to Port Authority provided equipment issues and/or failures;
(e) Failures caused by a 3rd party; or
(f) Act of God.

Should a failure occur in the system that is caused by hardware failure, it shall be repaired and the test resumed with downtime accrued. Where the failure causes inadequate test data to be collected or a loss of test data, then the test shall be restarted from a point where it can be successfully completed with data to verify compliance with the Contract and the test procedures document.

If the system "crashes" during a test, then the test shall be stopped. "Crash" is defined as a failure in which the PARCS cannot properly process revenue transactions. The Contractor shall analyze the cause of the system "crash," document the cause in a system problem report, responsively repair the flaw, document the repair in a corrective action report and record the downtime.

Where corrective action impacts delivered documentation, the documentation shall be corrected prior to final acceptance. Only after Contractor has repaired flaw and Port Authority accepts corrective action and the flaw report can the test be restarted.

Upon formal written approval of the corrective action report by the Port Authority, testing may continue if a problem has been encountered as long as the Contractor can clearly demonstrate that the failure is associated only with one function of the system, corrective action has been taken to remedy the failure, and the corrective action shall not impact other areas of the system.

Where the system does not perform a function or incorrectly performs the function but the system does not crash, testing may continue, as long as the function is corrected and all of the following conditions are met:

(a) the functionality of entry/exit lanes and parking time works properly according to the Contract,
(b) the functionality of parking fee calculations and correct collection works according to the Contract;
(c) no personnel, vehicle or driver safety issues exist;
(d) transactional archiving operates in accordance with the Contract;
(e) failure does not cause loss or contamination of transactional data; and
(f) all reports balance and are 100% accurate.

Where the above criteria are not met, the test shall be stopped and corrective action taken and verified prior to testing restart.

During the test, the continued availability of the system shall be demonstrated. Where a failure occurs that causes data loss, system instability (crash), and/or contamination of the transactional data and the database, the Contractor shall immediately correct the problem. Testing shall continue until a consecutive 30-day period of stable operation is achieved. Stability is defined as the proper functioning of the PARCS with a failure having no impact on the continued system operation or on the integrity of transactional data.

(1) Performance Period

The Operational Acceptance Test shall begin on the date of notification of the Contractor by the Authority to commence Operational Acceptance Testing and shall end when the PARCS has met the technical specifications set forth in the Operational Acceptance Test Plan approved by the Authority.

(2) Failure to Complete Acceptance Testing Successfully

In the event the PARCS is deemed not to have successfully completed one or more of the required Operational Acceptance Tests within ninety (90) days of their scheduled completion, then the Authority may, at its sole discretion, pursue any remedy hereunder or available at law or in equity or seek to enforce any damages, including but not limited to the Authority requiring the Contractor to install, within such time period as may be mutually agreed upon in writing by the Authority and the Contractor, a direct substitute of equipment or components. The Contractor shall use due care in the removal and substitution of such equipment or components. Such substitutions shall be subject to Acceptance Testing as provided in this section.

(3) Punch List

Starting with the first week after completing the FAT through final system acceptance, the Contractor shall submit a document on a weekly basis showing

the status of all outstanding system issues, regardless of severity, including the plan for resolution and estimated completion date.

e) Final System Acceptance

Final System Acceptance will be submitted by the Port Authority, in writing to the Contractor, upon successful completion of the FAT, all LATs, all Site Acceptance Tests, the OAT, upon verification by the Port Authority of complete resolution of all outstanding items on the punch list, receipt of detailed Record Drawings, and independent Qualified Security Assessor validation that the installed system is PCI-DSS compliant.

i) Close-Out Documentation

Upon Authority acceptance of the completion of the Thirty (30) Day Operational Acceptance Test, the Contractor shall prepare all materials necessary to close out the design and installation portion of the Contract. This shall include but not be limited to: the delivery of a fully functioning PARCS that meets all Contract functional and performance requirements and that has successfully completed Factory, LATs, SATS and Operational Acceptance Testing; the delivery and approval of all documentation and; the training of all management, supervisory, operations, system administration and maintenance staff, as specified in the training plan. The Contractor shall have transferred to the Authority at the end of the Thirty (30) Day Operational Acceptance Test, all documentation that is necessary for the operation of the PARCS whether or not it has been submitted as part of a previous deliverable. This includes but is not limited to: third party software documentation and licenses, software executable code, hardware documentation, a complete inventory report of all hardware with serial numbers and all software and maintenance manuals. At the end of the Thirty Day (30) Operational Acceptance Test, the Contractor shall deposit the Close-Out version of the Revenue Control System source code, software, development tools and documentation listed in the Escrow Agreement.

ii) Additional Requirements

The Contractor shall install all hardware, infrastructure, communications equipment and systems provided under this Contract in accordance with local building codes, (NYC Construction Codes for JFK and LGA, New Jersey Uniform Construction Code for EWR, New York State Uniform Fire Prevention and Building Code and State Energy Conservation Construction Code for SWF) and the National Electrical Code (NEC). The Contractor shall furnish all labor, tools, and supplies required to install all equipment and systems. Contractor shall remove all debris at no additional cost to the Authority. Any requirement for additional power will be at the Authority's expense.

The Contractor shall be responsible for field locating the closest available existing source of 120 volt power for each equipment item. The Contractor shall define its times and method of equipment delivery, which is subject to the Authority's review and approval.

The Contractor is required to submit a system implementation phasing plan for the Authority's approval within one hundred twenty (120) days of Contract execution, and prior to the start of any installation or construction work in the project areas. The Contractor may work on installations at multiple airports simultaneously. At each airport, the redundant host configuration shall be launched first, and then the PARCS field components may be installed. Once the system at an airport is fully operational, the Contractor shall launch that system without waiting to complete the remaining airports' systems.

iii) Prosecution of Work

Upon commencement of installation work, the Contractor shall make all efforts to complete the work in the scheduled amount of time approved by the Authority in the phasing plan. In the event the Contractor fails to meet those schedules, additional shifts, as required, including Saturdays, Sundays, and Holidays shall be scheduled to complete the work at no additional cost to the Authority.

iv) Non-Performance of Services

The Contractor shall perform the work at such times and places and in such a manner as the Program Manager shall direct or approve in accordance with the terms and provisions hereof. The Contractor shall immediately, upon the direction of the Port Authority, correct all matters, which shall have been determined to be unsatisfactory hereunder.

13) SUBMITTAL SCHEDULE

a) Project Plan and Schedule

Within fifteen (15) business days after award, the Contractor shall submit a Project Plan and Schedule to the Port Authority's Project Manager. Elements of the Plan shall include, but are not limited to: installation plan drawings and product installation literature for all primary components of the System; a schedule and plan for the installation of all devices, communications conduit and cable, and computer hardware, development of custom software features and the loading of all software (with emphasis on what precautions shall be taken to minimize disruption of current operations); plans for the loading of the initial database; training; and, responsibilities for application administration during installation.

The Project Schedule shall include Gantt charts and PERT charts with the critical path identified (using CPM) showing when tasks occur, when resources are required, and what task dependencies exist. The Project Schedule shall be of sufficient detail and clarity so that all work can be reviewed and the Port Authority Project Manager can monitor progress. The charts shall indicate a logical sequence of work and identify all dependencies, personnel resources, material, equipment, and work areas required for completion of the work. The Project Schedule shall be submitted both electronically and hard copy.

The degree of detail shall be sufficient to identify at a minimum:

i) All activities, tasks and stages of construction, milestones and deliverables as specified both within the Contractor's system development and installation methodology and those specifically identified herein.
ii) All the activities and tasks associated with the development, installation, integration, configuration and preparation of the System and all subsystem components, submittals, testing and training.
iii) Project activities with associated tasks and sub-tasks.
iv) Interfaces and dependencies with preceding, concurrent, and succeeding work effort.
v) Resources needed and assignments down to the task level for staff, material, and equipment.

It shall be noted that the development, installation, integration and testing of all Technology Components shall be coordinated with the Port Authority Technology Department through the Port Authority Project Manager.

b) Progress Schedule - Preparation, Updating & Reporting

The Contractor shall prepare and submit updated progress schedules to the Contract Manager every other week, with a complete outline of all tasks and activities required for the execution of this project.

The Contractor shall also schedule and conduct regular status meetings on strategic, tactical and operational issues via telephone conference calls or at an Authority-selected site no less frequently than on a weekly basis with the Authority, and other service providers as necessary for resolution of agenda items. At the sole discretion of the Authority, the frequency of meetings may be adjusted. The purpose of these meetings shall be, (but not limited) to:

i) tracking the status of the work activities;
ii) reporting on the operational status of the services, infrastructure and communications links and availability of connectivity between the Authority and the

Contractor, as well as connectivity between end-users and the managed environment via the Internet and Mobile devices;

iii) reviewing and reporting on any operational issues including service tickets;
iv) reviewing the Contractor's performance to the contracted service level metrics;
v) reviewing Contractor's invoices for services provided;
vi) reporting or communicating on all availability of services and the environment directly impacting the Authority's services; and
vii) resolving disputes.

The Contractor shall produce and deliver to the Authority, at least 48 hours prior to each status meeting, an agenda that includes a status report listing strategic, tactical, and operational items and issues and the status of each. The report shall at a minimum provide a complete statement of the system's status through performance measure reporting, and indicate progress made on operational, project or task issues or activities during the reporting period. Also included should be progress made on work to correct deficiencies, the status of activities to be undertaken in the next reporting period, activities/tasks behind schedule and identification of problems/concerns related to the services, statistics on problems encountered/resolved in the reporting period and year-to-date, as well as statistics on the Service Levels (SLA) standards and ad hoc reports as required by the Authority. Service Level Agreements are described in detail throughout Section X., Maintenance of the System.

c) System Diagrams

Within twenty-one (21) days after Contract Award, the Contractor shall submit to the Port Authority's Project Manager for review and approval the following detailed system design documentation:

i) System Block Diagram illustrating the interrelationship between all system components.
ii) Connectivity Diagrams to illustrate the connections among all system components including, but not limited to, the primary and backup application and database servers, Workstations, communications network and any proposed external connections. The connectivity diagram shall identify the use of all ports and communications protocols.
iii) Schematic diagrams to show the proposed locations of the equipment that are to be furnished and installed.

d) Security Practices and Policies

Within ten (10) days after Contract Award, the Contractor shall submit to the Port Authority's Project Manager a description of all system security features, practices and policies that are designed into the System to protect, control and monitor access to the

System and its components (e.g., hardware, software and data) to achieve the security requirements as described herein.

e) System Design Documentation

System Design Documentation shall be provided to the Authority in accordance with an approved project schedule. System Design Documentation has five (5) major components; system documentation, hardware documentation, computer software documentation, computer hardware documentation and Communications Network Architecture documentation as described in the following paragraphs:

i) System Documentation

The Parking Access and Revenue Control System Documentation shall include:

(1) Executive Summary: a summary of documentation material provided in this deliverable, an overview of the entire system describing all major components of the Parking Access and Revenue Control System, and special features of the Parking Access and Revenue Control System, which address performance, expansion, system security, ease of use, and maintainability.
(2) Design Overview: a description of the overall design. This shall include the advantages and disadvantages of the design, (e.g., modularity, fault tolerance/redundancy, flexibility, expandability), and an explanation of why the design is the best implementation to meet the Authority's requirements.
(3) System Architecture: a system-level graphic representation of all hardware components and their interconnections. This shall include identification of the interfaces between each device and computer, including direction of data flow (where data is initiated from), ports and protocols used for each connection.
(4) System Processing Narratives: detailed narrative descriptions of each major processing activity to be performed by the Revenue Control System. The narratives shall describe how all equipment and software interact to satisfy the functional requirements of the Revenue Control System. These narratives shall be a clear and comprehensive explanation of how each of the Authority's functional requirements are supported by the Revenue Control System.
(5) Security Features: a description of all system security features, computer controlled and physical, designed into the Revenue Control System to control and monitor access to the Revenue Control System and its components (e.g., hardware, software and data).
(6) System Reliability: an analysis of system reliability based on the Mean Time Before Failure (MTBF) and expected Mean Time to Repair (MTTR) for each major component and subsystem, including calculation methods and support documentation. If the configuration requires redundant or high availability components or equipment, the Contractor shall also provide a description of the

hardware and/or software features incorporated to meet the requirement for high availability in the event of the failure of one or more system components.

(7) Failure Handling and Recovery: a failure / recovery matrix showing the types of failures, the process of reporting these failures and if automatic or semiautomatic. This shall include descriptions of system diagnostics to detect and isolate failures.

ii) Hardware Documentation

(1) Equipment Submittals

For all equipment, the Contractor shall submit system level block diagrams that demonstrate the feasibility of the system as well as the interconnection of all equipment. The Contractor shall include in the block diagrams, the electrical and mechanical details and the interconnection details showing equipment part numbers, cable type, connectors, etc. The Contractor shall use separate sheets for subsystem and complete system configurations. The Contractor shall include block diagrams for every major functional area.

The Contractor shall provide descriptive material (manuals, cut- sheets, drawings, brochures, etc.) for each type of equipment and apparatus proposed to demonstrate that the intended equipment or integration of intended equipment will meet the functional objectives of the System. Where applicable, depict rack enclosure equipment layouts, including dimensions of rack and components. The Contractor shall include in these documents sufficient technical data for complete evaluation of the proposed equipment and system by the Authority. The Contractor shall describe the quality, function and capability of each deliverable item.

(2) Equipment Documentation

The Contractor shall provide complete operating, maintenance and installation manuals for each type of equipment item specified herein. The manuals shall include sufficient information for the Authority to fully operate and maintain the equipment including schematic wiring and interconnection diagrams; complete instructions for proper installation including equipment outlines, mounting, a complete parts list and a list of recommended spares.

The manuals shall include text that describes all functional capabilities of the equipment; explain all adjustments; how they are performed and their effect on equipment operation. The manuals shall include flow charts that describe troubleshooting procedures in a logical manner. The manuals shall describe required test equipment and incorporate descriptions of its use in manual sections dealing with maintenance and repair of the equipment items.

The manuals shall include information necessary for the proper installation, start-up, initialization and operation of the equipment item.

The manuals shall include environmental and operational specifications such as operating temperature range, power requirements, equipment weight, special handling considerations and equipment power dissipation rates and cooling requirements.

(3) Computer Software Documentation

The Computer Software Documentation shall include:

(a) Software Architecture: system-level illustrations, such as flowcharts and block diagrams, illustrating the overall structure of the Parking Access and Revenue Control System software. These diagrams shall include the major processing functions performed by each subsystem or major module, their interaction with each other and with the Parking Access and Revenue Control System user.

(b) Software Configuration: a description of the operating system, application, database/data management, utility, graphical user interface, device drivers and any other software used in the Parking Access and Revenue Control System. The Contractor shall identify which software is to be custom developed and which is third party software. For third party software, the Contractor shall explain the functions to be performed by the product and identify the manufacturer, version and release to be used and shall submit all technical specifications and literature (e.g., user and system documentation, brochures, and any other literature produced or customarily provided by the third party manufacturer). For custom software, the Contractor shall identify the languages, compilers and utilities to be used (including version and release number) in development and operation. For all proposed third party software, copies of the associated license agreements shall be submitted for approval.

(c) Database and Data Management Structure: a description of the overall organization of the files and/or database to be used in the Revenue Control System. This description shall also include, but not be limited to, full details regarding any third party database products including version, release, functional characteristics, operational requirements, and any other relevant characteristics of the product. The Contractor shall submit a schema of the logical relational structure.

(d) Data Dictionary: a listing of all Revenue Control System data elements, including the size, definition, validation rules, purpose and other information pertaining to the data elements. If a commercially available data dictionary is to be used, the Contractor shall also submit complete and current information about the product.

(e) Data Storage Analysis: the techniques employed to ensure that the Revenue Control System can meet the storage requirements for on-line and historical data, and expansion capabilities. The analysis shall include identification of all files (e.g., system, message, report files), databases, and their retention cycles.

(f) Operator Interface: operator and user tools and techniques employed to ensure an easy to use, consistent and efficient interface between the operator and the Revenue Control System. Examples of such techniques are: the use of a graphical user interface, standardization in the formatting of screens and reports, consistent use of program function keys, color coded alarm notification, drop down, pop up menus, data porting and system monitoring of the Revenue Control System.

(g) Program and Module Narrative: a description of major program modules contained in the Revenue Control System and a description of the processing functions, inputs and outputs of these modules. Particular emphasis shall be placed on customized application software.

(h) Detailed Software Design: block diagrams, flow charts and/or other software design documentation that describe the design of the Revenue Control System software by major subsystem. This information shall include the details of main processing functions performed by each program or module, including inputs, outputs, and data type definitions.

(i) Inputs and Outputs: a description of all the Revenue Control System inputs and outputs. For inputs, describe all transactions, messages, records, signals, etc. to be received. For outputs, identify screens, reports, menus, etc. that are produced or presented to the end user (operator, supervisor, administrator). Contractor shall provide the documentation for field structures of messages and records and the methodology for redefining menu structures.

(j) System Performance Analysis: an explanation of the capability of the Revenue Control System to meet the performance requirements. The Contractor shall fully describe, explain and document the analysis that was used to support its statements of performance, durability, and availability. Where such documentation relies upon third party manufacturer claims,

promises, or warranties, or relies upon the claims, promises, or warranties of the manufacturer's marketing or sales representative, the Contractor shall submit copies, or, as appropriate, original documentation of said promises, representations, and warranties. The Contractor shall provide complete product information for any automated tools used in this analysis.

(k) Redundancy: an explanation as to how the system will ensure continued full functionality should a server or data repository suffer a failure. The Contractor shall describe planned connections to more than one data reporting network appliance.

(4) Computer Hardware Documentation

The Computer Hardware Documentation for equipment furnished and installed by the Contractor, shall include:

(a) Hardware Specifications: a full bill-of-materials and complete specifications (e.g., make, model, environmental and power requirements, ratings, expansion slots, communications ports, etc.) for each computer hardware element of the Revenue Control System. Hardware specifications must include an expansion of equipment functionality and theory of operation.

(b) Component Drawings: drawings that clearly and completely indicate the function of each Revenue Control System hardware component. The drawings shall indicate termination points of devices, and interconnections required for system operation, interconnection between modules and devices, spacing of components, and location, mounting and positioning details.

(5) Communications Network Architecture

The Communications Network Architecture shall include:

(a) The Contractor shall provide detailed diagrams and full technical specifications of communications network components, hardware and software, and communications protocols and network topologies used in the Revenue Control System architecture.

(b) The Contractor shall also provide a system-level diagram of the communications network and specifications for each major component and identify how the component functions in the network, direction of data flow, ports and protocols for each connection. Network diagrams shall include Revenue Control System communications diagrams detailing the wiring and interconnections between the Revenue Control System and other devices.

The Contractor shall describe the techniques employed to ensure that the network can meet the volume of transaction traffic to be supported and is capable of meeting performance and expansion requirements.

(6) Operating Documentation

The Contractor shall provide all documents, manuals, and printed materials necessary for the effective operation of the Revenue Control System. The documents provided shall be in bound copies. Additionally, an electronic version shall be provided using an industry standard word processor, such as the most current version of Microsoft Word for Windows. This documentation shall be written in a clear concise manner, and shall cover every component of the system that an operator, administrator, technician, auditor and management would need to know to fulfill their roles in the operation and maintenance of the system. This will include, but not be limited to, the following specific Manuals:

(a) Standard Operating Procedures Manual

A Revenue Control System Operating Procedures Manual shall be provided which contains graphical depictions and explanations of system operation for all operator/cashier/supervisor/audit functions. This manual shall be for instructional, study and refresher use and shall explain all the features and functions of the Revenue Control System for day-to-day operation (e.g., log-on, monitors, print daily reports). The manual shall also have a section for problems and/or exception conditions so the operator can resolve common operating problems (e.g., trouble shoot network problems, restart the Revenue Control System in the event of a component failure, clear jams). The manual shall also contain instructions on how to perform normal maintenance (e.g., changing paper for the printer). This Manual shall be submitted for approval not later than forty-five (45) days prior to commencement of the formal Training Program.

(b) Reports Manual

A description of all standard reports including but not limited to:
(i) Purpose of report
(ii) What selection options are available
(iii) Sample report layout
(iv) Description of all fields shown and what they mean
(v) Instructions on how to access all reports from a workstation.
(vi) Instructions for authorized personnel on how to create, identify and add custom reports.

(c) Emergency Operating Procedures Manual

An Emergency Operating Procedures Manual shall be provided which contains graphical depictions and explanations of system operations for all emergency functions specified under Operator Training. This manual shall explain all the features and functions of the Revenue Control System for emergency operations. This Manual shall be submitted for approval not later than forty-five (45) days prior to commencement of the formal Training Program (see below).

(d) System Administrator Procedures Manual

A System Administrator Procedures Manual shall be provided which contains graphical depictions and written descriptions of all functions. This manual shall contain all procedures necessary for the proper monitoring and administration of the enhanced Revenue Control System. At a minimum, the manual shall contain separate sections that cover the following topics: startup and shutdown procedures, instructions for cold start of system equipment, backup and recovery, performance analysis, scheduled maintenance, user management, audit and control, report production, configuration control, system diagnostics, database integrity, special requests and expendable supplies. A separate, removable section of the System Administrator Procedures Manual shall contain information on the proper administration and control of the security features built into the Revenue Control System. Some of the information to be contained in this section include: maintenance of user identifiers, password control, and security policy review. Information on appropriate review of security controls for adherence through various types of reporting mechanisms and utilities and/or third party security software. This Manual shall be submitted for approval not later than forty-five (45) days prior to commencement of the formal Training Program.

(e) Supervisor Procedures Manual

A Supervisor Procedures Manual shall be provided with graphic descriptions of all functions and procedures required for system modifications specified under supervisor Training. This manual shall contain all the instructions included in the Operator Procedures Manual plus instructions on printing standard and ad hoc reports. This Manual shall be submitted for approval not later than forty-five (45) days prior to commencement of the formal Training Program.

(f) Site Specific Manuals

Site specific manuals shall be provided which shall include, but not be limited to, the following: site specific configuration parameters; detailed system

configuration narratives; default parameters, actions, and descriptors; and device and component addresses and locations. This Manual shall be submitted for approval not later than forty-five (45) days prior to commencement of the formal Training Program.

(7) System Design Review

Contractor shall submit necessary documentation to conduct a Conceptual System Design Review (CSDR), Critical Design Review (CDR) and Software Development Review (SDR) for the New PARCS, in that order. Required documentation and all hands-on use of the PARCS shall demonstrate to the Port Authority that, at minimum, the Contractor's proposed system meets 100% of the requirements of this specification. The Contractor shall be responsible for updating the Requirements Matrix, submitted with its proposal, to ensure it is accurate and complete. The Port Authority shall require a minimum of fifteen (15) business days for the review of each system design. To receive written acceptance, Contractor shall incorporate and demonstrate the Port Authority's feedback/comments from CSDR and CDR prior to commencement of the next milestone review. Contractor shall not proceed with the next design requirement until receipt of written acceptance presented by the Port Authority. The following summarizes in detail the requirements of these reviews:

(a) Conceptual System Design Review (CSDR)

Thirty (30) calendar days prior to the CSDR, the Contractor shall submit for the Port Authority's review and approval a CSDR Plan that includes the time, place and length of the review; review format; overall description of review; goals of the review; agenda items and topics; recommended participants; and the role/responsibilities of Port Authority personnel in the review.

Any Port Authority comments and approval will be granted prior to twenty (20) calendar days prior to the CSDR.

Fifteen (15) calendar days prior to CSDR, the Contractor shall submit twenty (20) copies of the CSDR documentation as well as electronic copies, including all Port Authority feedback and comments, to the Port Authority for review. Documents to be submitted shall include, but not limited to, the following:

(i) Overall description of the PARCS and system components
(ii) System schematics, block diagrams, interconnection diagrams, and flow charts
(iii) Specifications or cut sheets for all proposed components and installation procedures
(iv) Standard reports samples and proposed formats for new reports

(v) Software design approach, database design and list of all software
(vi) Detailed description of proposed credit card data flow and processing.
(vii) Operational flow chart or sequence of activities diagram
(viii) User screen formats
(ix) Transition Plan
(x) Test scripts for all systems components operational procedures; and
(xi) Detailed description of each activity, functionality, and operation, described in sequence and encompassing all system hardware and software components.
(xii) Contractor shall facilitate and conduct the CSDR at Port Authority offices or at a location approved by the Port Authority.

(b) Critical Design Review (CDR)

Thirty (30) calendar days prior to the CDR, the Contractor shall submit for the board review and approval a CDR Review Plan that includes the time, place and length of the review; review format; overall description of review; goals of the review; agenda items and topics; recommended participants; and the role/responsibilities of the Port Authority in the review.

Any Port Authority comments and approval will be granted prior to twenty (20) calendar days prior to the CDR.

Fifteen (15) calendar days prior to CDR, the Contractor shall submit twenty (20) copies of the CDR documentation as well as electronic copies, including all Port Authority feedback and comments, to the Port Authority for review. Documents to be submitted shall include, but not limited to, the following:

(i) Detailed description of PARCS and system components
(ii) Completed schematics, block diagrams, interconnection diagrams, interface plans, interface control documents, and system and subsystem flow charts
(iii) Detailed specifications and/or manufacturer's cut sheets for all proposed components
(iv) Detailed installation procedures
(v) All standard and new reports
(vi) Procedure to add reports
(vii) Detailed software design documentation
(viii) List of all hardware necessary for initial operations
(ix) Spare parts inventory
(x) Detailed central server system, network and communications design documentation. This shall include the following:
(xi) A recommended server architecture
(xii) Server hardware requirements

(xiii) Network port density and bandwidth requirements
(xiv) Operations Plan describing and detailing end-to-end operations of the system
(xv) Maintenance and servicing procedures for system components
(xvi) Graphical User Interface (GUI) User Screens
(xvii) Detailed and phased testing plan including both internal and Port Authority observed; and
(xviii) All software and database documentation including, but not limited to, licensing information and agreements, system and subsystem block diagram schematics, data flow diagrams and structures.

(c) Hands-on Technology Department Workshop

As part of the CDR, the Contractor shall meet with Port Authority Technology Department (TEC) staff to review the Contractor's recommended system architecture, identify the Contractor's detailed requirements for the new computing and networking platform, and work cooperatively with TEC staff to finalize a complete, new system architecture, server and network design that accomplishes the following:

(i) Meets the functional and performance requirements stated by the Contractor and agreed to by TEC
(ii) Complies with the referenced Technology Standards for the Port Authority in Attachment K;
(iii) Complies with the current version of the PCI standards;
(iv) Complies with the requirements stated in the Audit Control List:
(v) Creates a redundant, diversely located computing and network environment that supports load sharing and automatic failover; and
(vi) Complies with the data retention requirements described herein.

Once concurrence is reached for the system, server and network architecture, the Contractor shall submit for Authority approval, a complete system design that shall include, at a minimum, the following items:

(i) System network diagrams that depict the proposed system architecture illustrating all communications, physical and logical locations of equipment, the direction of data flow, the ports that will be used and their communications protocol.
(ii) System design documents that describe the data flow reflected in the new system architecture, and identify the detailed requirements for the new servers to be built, and required networking connections to resources.

As part of project implementation, the Authority shall build the server infrastructure based on the agreed-upon server architecture and provide the Contractor with access to the servers to install its software.

Contractor shall facilitate and conduct the CDR at the Port Authority or at a location approved by the Port Authority. The CDR shall address those system design documents listed above as well as hands-on use and evaluation of the PARCS for no less than a five (5) business day period by Port Authority.

(d) Software Development Review (SDR)

Thirty (30) calendar days prior to the SDR, the Contractor shall submit for Port Authority review and approval an SDR Review Plan that includes the time, place and length of the review; review format; overall description of review; goals of the review; agenda items and topics; recommended participants; and the role/responsibilities of Port Authority personnel in the review.

Any Port Authority comments and approval will be granted prior to twenty (20) calendar days prior to the SDR.

Fifteen (15) calendar days prior to SDR, the Contractor shall submit twenty (20) copies of all SDR documentation as well as electronic copies, including all Port Authority feedback and comments, to the Port Authority for review. Documents to be submitted shall include, but not limited to, the following:

(i) Description of all software and firmware for all programs and subsystem, including data flow and data structure diagrams, database documentation, and software inter-relationships and integrations
(ii) Detailed description of each program, program function and operation
(iii) Files and message formats
(iv) GUI and user screen layouts, contents and formats
(v) Documentation for all object-oriented software including application specifics, object diagrams, event coding, and relationships
(vi) Documentation for all command, batch, script or other files used to compile, link, load and/or execute application software and/or firmware
(vii) Operating systems, communication programs, assemblers, compilers, and utility programs used in the PARCS
(viii) Software Contractor’s standard manuals
(ix) Software maintenance plan including all routine, preventive, corrective and remedial maintenance and servicing procedures and commands
(x) All standard and new reports
(xi) All other pertinent software and database development issues and documentation including, but not limited to, licensing and ownership

information, user manuals, system administration manuals, and any other software agreements or manuals.

Contractor shall facilitate and conduct the SDR at the Port Authority or at a location approved by the Port Authority. The SDR shall address those software development documents listed above as well as the following:

(i) Real-time, hands-on PARCS demonstration of all software programs, commands, functions and screen formats
(ii) Hands-on use and evaluation of the PARCS for no less than a five (5) business day period by Port Authority.

14) APPLICATION SYSTEM DOCUMENTATION

The Contractor shall establish and maintain a documentation library containing all hardcopy and computer readable documentation for software developed during ongoing maintenance. The Contractor shall be responsible for ensuring that all documentation needed for the continued operation and management of the PARCS is accurate, current and available and is in compliance with, at a minimum, a structured maintenance methodology acceptable to the Authority. All application software, documentation, and instruction for reconstitution remains the property of the Authority, and all physical documentation must be maintained on site at the Authority, and not removed from its premises. Four (4) copies of application source, object, tools to rebuild system, and third-party system, documentation and method to reconstitute the system must be provided to the Port Authority.

The scope of the system documentation portion of the application support services furnished shall include but not be limited to the activities identified below.

a) Manuals

Within twenty-one (21) calendar days prior to the start of the Factory Acceptance Test, prepare and submit, for approval, ten (10) sets of complete, separate manuals for Authority review and approval. Site-specific manuals shall also be provided to document the specific site-related configurations and operations / maintenance. Additionally, all Manuals shall be available electronically.

i) Operations Manuals

A set of Operations Manuals shall be provided that clearly describes all User operations. The manuals shall explain all the features and functions of the PARCS for day-to-day operations and how to use the system to manage more complex situations. A separate Quick Reference Guide for problems and/or exception conditions shall be included to enable the User to quickly resolve common operating

problems, and address common configuration and replay techniques. The Quick Reference Guide shall be available in multiple locations; one source shall be within the electronic and hard copy Operations Manual and the other as a stand-alone electronic and hard copy version of the document.

The Operations Manual(s) shall contain detailed description of system operations and procedures on how to perform all user functions, including but not limited to the following: Monitor equipment operation, Control all equipment (if applicable), Invocation and explanation of the PARCS reports, Filter and sort the event log, Implement any special system features, and Error and alarm handling procedures, including recovery from all equipment failures.

The Operations Manual shall be written for beginner computer users who are not familiar with detailed computer operations and terms. It shall contain step-by-step procedures with examples containing pictures of the computer screens, explanation of the user interfaces and graphics to illustrate the overall concepts. The Operations Manual shall be for instructional, study and refresher use.

ii) Application Administration Manual

The Application Administration Manual shall include, but not be limited to all sections covering administration of the application, configuration functions, including but not limited to the following items:

(1) Detailed instructions and procedures for the installation and configuration of the software;
(2) Detailed description and procedures for configuration of user access privileges and access levels to use of all application functions;
(3) Detailed description and procedures for the configuration and management of the application and its databases;
(4) Detailed description and procedures for installing, backing up and restoring the application software and include system generation procedures if software development tools are furnished as part of the Contract;
(5) Detailed description and procedures for event logs maintenance activities including downloading, sorting, printing and clearing;
(6) Detailed description and procedures conducting system health check to ensure the operational health and vitality of the system; and
(7) A detailed procedure that describes all of the steps to manually switch over operation from the primary application and database servers to the backup application and database servers and to switch back to the primary application and database servers once the operation of the primary application and database servers are restored.

iii) System Administration Manual

A System Administration Manual shall be provided, which contains graphical depictions, written detailed descriptions and procedures of all functions that the Contractor will perform for the proper monitoring, maintenance and administration of the PARCS, including but not limited to, the following topics, each described in a separate section of the document:

(1) steps to manually switch over operation from the primary Servers to the secondary servers and to switch back to the primary servers once the operation of the primary servers is restored
(2) archiving data and restoring archived data to the database
(3) backing-up and restoring the database
(4) changing the database to add or delete tables and or fields; installation and configuration of the software
(5) backing up and restoring the application software and configuration files
(6) generating the system software from the source code
(7) performance analysis
(8) scheduled maintenance
(9) audit and control
(10) report production
(11) contingency plan and procedures
(12) configuration control
(13) system diagnostics
(14) database integrity checks
(15) Network problem determination

A separate, removable section of the PARCS System Administration Manual shall contain information on the proper administration and control of the security features built into the System. Some of the information to be contained in this section includes: maintenance of user identifiers, password control, classes of users, class permissions and security policy review.

b) Audit Report

Prior to the completion and acceptance of the Factory Acceptance Test, the Contractor shall obtain and submit, for the Port Authority's approval, an internationally recognized certification (such as SSAE 16 SOC 2 Type 2 or an approved equivalent) of the security policies and practices employed in its System operation which demonstrate that the following protections are provided:

i) Logical access to the production environment, data files, and sensitive system transactions, is restricted to authorized users only
ii) Regularly scheduled processes that are required to maintain continuity of operations in the event of a catastrophic loss of data, facilities, or to minimize the impact of threats to data, facilities or equipment, are performed as scheduled.

iii) System hardening measures have been adequately applied to protect PARCS against risks to which it is exposed
iv) Logging of IT security events is enabled for PARCS, security logs are reviewed in a timely manner, and appropriate actions are taken by Contractor IT staff in response to System security events.

c) Change Management

Prior to the start of the first Lane Acceptance Test, submit the form that will be provided by the Contractor and the procedures that will be performed, for Authority approval, before attempting to effect a change to any part of the production system, whether hardware, software, database or network. This form shall include, at a minimum, the information contained in the attached Change Control Submission form (See Attachment Q).

d) Database Documentation

Prior to the start of the first Lane Acceptance Test, the Contractor shall submit to the Port Authority's Project Manager for review and approval a detailed description of the database. Database documentation shall include:

i) Database Schema

Database schema is a description of the overall organization of the files and tables to be used in the PARCS. This description shall include an identification of all data files, tables, and fields, and the relationships between fields and tables and demonstrate compliance with the data requirements specified herein. This description shall also include, but not be limited to full details regarding any third party database products including version, release, functional characteristics, operational requirements and any other relevant characteristics of the product.

ii) Data Dictionary

A listing of all PARCS data elements, including the size, definition, validation rules and other information pertaining to the data elements. If a commercially available data dictionary is to be used, also submit complete and current information about the product.

iii) Data Storage Analysis

The techniques employed to ensure that the PARCS can meet the storage requirements for on-line and historical data and expansion capabilities. The analysis shall include identification of all files (e.g., system, message, report files), databases, and their retention cycles and indicate the accessibility to the data, i.e. whether the information will be available for on-line retrieval or archived in off-line storage.

iv) Data Flow Diagram

A graphical depiction of the logical processes that comprise the PARCS and an illustration that depicts the data flow as the data moves between these processes. This description shall identify all of PARCS functional processes and show the flow from the data's inception to its long-term storage. The documentation shall include data flow diagrams and other necessary documentation to understand how the data is processed and stored.

v) Entity-Relationship Diagram

A graphical illustration of the interactions between the various entities for which data is collected in the PARCS that depicts the relationships between the entities and their associated data. This description shall identify all significant PARCS entities (person, object, place, events, etc.) and show the nature of all significant interactions from the data's inception to storage.

e) Final Versions of the Documentation

Prior to certification by the Authority that the Contractor has completed all work as specified in the Detailed Project Plan (except for maintenance), the Contractor shall submit all design documentation, manuals, and/or drawings, which have been revised to reflect the as-built conditions. System Documentation shall be provided in both a bound copy and an electronic version in a machine-readable form, which is viewable with currant Microsoft Office suite of tools and Auto-Cad (if used). System documentation submittal(s) shall include but not be limited to versions of the System Drawings and System Documentation that have been updated to reflect the as-built conditions.

i) Establishing Documentation Library

The Contractor shall maintain a documentation library containing all documentation material for software, standards manuals and procedure manuals, and shall obtain or produce necessary documentation not in the PA's possession. All material in or obtained for the documentation library shall be the property of the Authority. Where documentation does exist, the Contractor shall ensure that, at a minimum, it meets documentation standards as set in the Contractor's structured maintenance methodology, as accepted by the Authority. The Contractor shall work with the Authority to ensure that controlled access to documentation materials is maintained, signing out manuals to authorized individuals when appropriate and tracking the location of signed out materials. In a similar manner, access to electronic versions of documentation shall also be controlled at the user ID level. In

addition, the Contractor will provide an annual review/assessment of the document library.

ii) Archiving Data

The Contractor shall follow System archiving procedures to capture data to be archived to permanent storage media as required to maintain proper System functioning or as scheduled in the System operating procedures (whichever occurs first), for the systems that are not administered by the Authority's system administrator . The Contractor shall ensure that archived media is properly stored, logged and maintained and that archived data is viable and accessible throughout the required archive retention period for the data and test that the media is viable and contains the archived data on a quarterly basis.

The Contractor shall also be responsible for ensuring that an adequate inventory of media for primary and backup purposes is available and for providing additional media when needed in a timely manner. The Contractor shall be responsible for loading archived historic data onto the System as needed to generate reports; and for doing required searches and clearing loaded historic data when it is no longer needed for immediate, on-line access.

iii) Maintaining Application System Documentation

The Contractor shall maintain a run book for Computer Operations as well as a functional specifications document describing the business purpose of the System and a high-level description of the processes and reports; a design specifications document detailing the technical solution to the business function described in the functional design document described above; and maintain program documentation including narrative descriptions, specifications, configuration, code listings, data layouts, IPO (Input, Processing, Output) charts, flow charts, etc. All applicable documentation shall be put in escrow.

iv) Maintaining Test Plans

The Contractor shall maintain test plans and procedures, acceptable to the Authority, for retesting the System after modifications to base software, applications, and/or databases. The Contractor shall also maintain a file of all test results in accordance with the documentation standards referenced herein and evaluations of results along with any recommendations resulting from testing. All test plans and related files and data shall be the property of the Authority. Test plan documentation shall include but not be limited to:

(1) Unit Testing - Create and maintain unit test plans to verify the functioning of the new and/or modified System component, and that it satisfies the business user's requirements.
(2) System and Integration Testing - Create and maintain test plans to test the entire System with the new and/or modified component installed to verify the integrity of the System as a whole and to determine that the intended purpose of the new and/or modified component is achieved.
(3) Acceptance and User Testing - Create and maintain test plans to verify the functionality of the new and/or modified component in the production environment for a specified period, prior to final acceptance.

15) SERVICE LEVELS AND LIQUIDATED DAMAGES

The Contractor's obligations for the performance of all Work at the service levels, as described herein, specified in this Contract are of the essence. The Contractor guarantees that it can and will complete performance under this Contract at the service levels stipulated herein.

The Contractor's obligations for the performance and completion of the work within the time or times provided for in this Contract are of the essence of this Contract. In the event that the Contractor fails to satisfactorily perform all or any part of the work required hereunder in accordance with the requirements set forth herein or the signed Contract and to the extent that such damage and loss to the Port Authority for such failure to perform includes amounts that are difficult of accurately quantify, the damages to Port Authority shall be liquidated in the following amounts:

Category	Service	Service Level	Liquidated Damages in the Event of Non-compliance
Application Maintenance *Attachment D, System Updates – NEW PARCS*	The application of all critical application and system patches and deployment of new software upgrades.	Contractor shall apply all critical application patches within 24 hours of their approval by the Authority. Software version upgrades shall be deployed within 12 months of general release by the application vendor and after Authority approval.	$500 per instance of non-compliance.
Application Response *Attachment D*	The time taken for the PARCS to complete a user request and return a response, measured from end-to-end. End-to-end time is measured from when a command or transaction request is entered to the time that the resulting actions are completed and displayed on the monitor.	Response time for the system to process a transaction at a lane, POF or workstation will be completed within 5 seconds for 90% of all transactions over a billing month.	2% of monthly support and maintenance costs for every 1% below target measured over the billing month.

Data Archiving *Attachment D, Archiving Data*	Archive data to preserve online storage and database performance.	Archiving shall be done at a frequency so that adequate server capacity is maintained 100% of the time. Contractor is also required to demonstrate successful recovery of backed up data on an annual basis.	1% of monthly support and maintenance costs for every instance of non-compliance.
Compliance *Attachments J and K*	Compliance with Audit controls and Technology Standards for the Port Authority.	The Contractor must satisfy 100% of requirements stated in Attachment J (Audit Department - Controls Requirement Contract Checklist) and Attachment K (Technology Standards for the Port Authority).	$500 for each item determined to be in non-compliance by the Port Authority Audit Department or Technology Department, per affected airport.
Data Integrity/ Currency *Attachment D*	Data integrity: the accuracy and consistency of the data and database structures. Data currency: the degree to which the data is timely and up-to-date.	Accuracy of all data entered through the application and stored on the database must be 100% at all times. All data must be 100% current 99% of the time over a billing month.	2% of monthly support and maintenance costs for every 1% under either target, to be measured over the course of a billing month.

Equipment Uptime *Attachment E*	The time that the fully functional equipment is available for use, excluding scheduled maintenance windows. Fully functional is defined as the equipment's ability to process all tasks and payment types for which it is designated, including cash, credit card, *E-ZPass®* and cell phone payments.	Each entrance plaza, exit plaza or POF bank shall be available and fully functional 99% of the time over a billing month.	$1,000 for every day, or part thereof, in which the metric is 1% or more under target.
		Each individual lane and POF shall be available and fully functional 95% of the time over a billing month.	$250 for every 1% under target for each day that the unit is out of service.

Application Availability *Attachment D*	The uninterrupted availability of PARCS Applications software.	100% availability of PARCS application software at all times. Can be satisfied as long as the applications software at each airport is fully operational on at least one host computer. Can also be satisfied if, in the event of the loss of host services, the elapsed time to fail over from primary to backup host does not exceed the fail over interval identified in the Attachment E, Functional Specifications. Loss of data shall be construed as a loss of the applications software availability for the period of time such data is unavailable.	$2,500 per affected airport for each day or part thereof that the host is unavailable, plus any lost parking revenue determined to have been caused by applications software unavailability as determined by the airport parking operator, the Port Authority Audit or Technology Department.
Hours of Service *Attachment D*	The presence of on-site contractor personnel during primary period of maintenance (PPM) at LGA, JFK and EWR	Contractor shall provide on-site service at the referenced airports from 8:00AM to 11:59PM, seven days per week. The Contractor shall provide the agreed upon amount of on-site personnel during the aforementioned time.	$50 per each unstaffed hour or part thereof per affected airport, in accordance with the staffing plan submitted accepted by the Authority.

Prebooking and Reservations	Web portal functionality to support customer reserved parking, promotional and prebooking capabilities.	Customer web portal must be fully functional 100% of the time: accessible to customers, able to fully process and complete parking reservation transactions and communicate with the PARCS applications software.	$500 per day or part thereof that the web portal is not 100% fully functional.

Problem Response/ Resolution *Attachment D*	Problem Response is the elapsed time between a service call (reporting a problem) placed by a user and the time contractor staff begin working on a solution.	During on-site hours (as specified above) Contractor must respond by phone to all service calls within 60 minutes of notification (JFK, LGA & EWR) or one business day (SWF). Contractor must respond to service calls received outside of on-site hours within 2 hours of notification (JFK, LGA & EWR) or two business days (SWF).	$250 per instance of non-compliance.
	Problem Resolution is the elapsed time between a service call (reporting a problem) placed by a user and a successfully implemented solution.	During on-site hours, Contractor must correct service call issues within 2 hours of notification (JFK, LGA & EWR) or two business days (SWF). Service requests received by Contractor outside of on-site hours must be corrected within 4 hours of notification (JFK, LGA & EWR) or three business days (SWF).	$250 per instance of non-compliance.

The above examples refer specifically to the work described hereunder, which is the Contractor's responsibility. The Authority shall actively monitor the Contractor's performance and enforce non-compliance and non-performance clauses by assessing liquidated damages as set forth herein. However, the Authority shall not assess liquidated damages if non-compliance and non-performance results from events or beyond the Contractor's control.

The Contractor shall track, calculate, monitor and report on performance against the Service Levels above and shall adjust invoices accordingly.

Repeated failure to meet the above Service Level Standards on the part of the Contractor constitutes a material breach of the Contract and may be cause for the Contractor to be declared in breach of Contract, regardless of the existence of liquidated damages provisions. In the event the Contractor is declared in breach of Contract, the Port Authority shall be entitled to collect liquidated damages up to the time of the declaration of breach, and actual damages arising from the breach suffered by the Port Authority after the declaration of breach.

16) MANAGEMENT OF THE WORK

The Contractor shall be responsible for the effective management of the work described herein and of the staff assigned to the work. The Contractor shall implementing sufficient management controls and utilize tools necessary to ensure that the work is accomplished in an effective, efficient manner.

a) Organization

The Contractor shall be responsible for establishing and maintaining an organizational and operational structure appropriate to the work to be performed under this Contract. This shall include but not be limited to:

i) Assigning an appropriate number of staff with requisite skills, acceptable to the Authority, for the tasks to be performed.
ii) Supplying direct supervision of the staff assigned to carry out the work as defined herein.
iii) Providing qualified persons, acceptable to the Authority, for relief of the assigned staff in the event of vacation, illness, personal business or any other absence of the assigned staff.
iv) Providing the staff assigned with procedures for escalating issues that cannot be solved on-site and providing for the support of these individuals where such support is required to ensure prompt resolution.

b) Labor Force

The Contractor shall furnish sufficiently trained management, supervisory, and technical personnel to perform the services required under the Contract, with all such personnel subject to review and approval by the Authority. Specifically, the relevant Contractor's staff assigned to the Authority under the Contract shall have achieved the following certifications by the commencement of the Contract:

i) MCSC License;
ii) MCTS;
iii) MCSD;
iv) MS SQL License

As part of its proposal, the Contractor shall include employee certifications.

Furthermore, such assigned staff shall maintain their certifications throughout the duration of the Contract in the application versions utilized by the Authority.

If any such personnel is deemed unsatisfactory or does not perform the services to be furnished hereunder in a proper manner and satisfactory to the Authority, or in the determination of the Director may have taken any action which constitutes a conflict of interest or which is inconsistent with the highest level of honesty, ethical conduct or public trust or which the Director determines is adverse to the public interest or to the best interest of the Authority, the Contractor shall remove any such personnel immediately from performing work under this Contract, and replace them by personnel satisfactory to the Authority within two weeks, upon notice from the Authority.

c) Status Meetings

The Contractor shall schedule and conduct regular status meetings with the Authority, at an Authority selected site, no less once per month. At the sole discretion of the Authority, the frequency of meetings may be adjusted, especially during the construction phase of the project where construction progress/coordination meetings shall be held at a minimum of weekly or biweekly. The purpose of these meetings will include but not limited to:

i) Reporting on the operational status of PARCS;
ii) Reporting/ on the construction progress/coordination of the new PARCS;
iii) Reporting on construction punch list items;
iv) Tracking the progress of application management activities;
v) Reviewing the Contractor's performance to the contracted service level metrics;
vi) Reviewing Contractor's invoices for services provided; and
vii) Tracking the progress of projects, work orders, etc.

The Contractor shall produce and deliver to the Authority, at least 24 hours prior to each status meeting, a project status report. At minimum, the report shall:

i) Provide a complete statement of the System's status;
ii) Include performance measure reporting;
iii) Indicate progress made during the reporting period;
iv) Indicate progress made on work to correct deficiencies, activities to be undertaken in the next reporting period, activities and/or tasks behind schedule;
v) Identify problems and concerns related to PARCS;
vi) Provide statistics on problems encountered and resolved in the reporting period and year-to-date.
vii) Provide Invoice tracking and expenditures.

d) Management Reports

See Attachment I for a list of required reports.

17) TRAINING

At the time of proposal, a Training Plan shall be provided by the Contractor in order to provide initial training for all users of the Parking Access and Revenue Control System. The Contractor shall conduct the required training at each of the four (4) facilities respectively, at the scheduled times and locations designated by the Authority consistent with the approved Training Plan. The full complement of training courses shall be conducted over time to accommodate shift personnel, vacations and make-up sessions. A detailed schedule for the delivery of all training shall be included in the Project Plan and Schedule and reported on during the regularly scheduled status meetings. All training shall be completed no later than fourteen (14) calendar days prior to commencement of the Field Acceptance Test at each facility. The training shall include, but not be limited to, the following groupings of staff with an estimated student population as shown.

Operator Training shall include a simulation of actual site conditions at each facility and shall be provided for one (1) group of six (6) students per course/per facility. Each group shall be trained for one (1) five (5) day instructional class. Training shall include but not be limited to: sequence of operation review; sign-on/sign-off; selection of all displays and reports; commanding of points, English and graphic mode; modifying text; reviews of all topics presented in the Standard Operating Procedures Manual.

The Contractor shall provide the necessary Standard Operating Procedures Manuals per facility for persons attending these instructional classes.

Upon completion of the training program at a facility, the Contractor shall prepare and deliver a training report, which shall summarize the results of the training program, including a list of attendees, course evaluation form, and recommendations for follow-up training or modification to the curriculum.

a) Training Plan

At the time of proposal, the Contractor shall provide a sample Training Plan. Within one hundred twenty (120) days of the passing of the Factory Acceptance Test, the Contractor shall provide for the review and approval of the Port Authority a Training Plan, consistent with the plan originally proposed and accepted, which shall address Operator Training, Supervisor Training, System Administration Training and Maintenance Training. As part of the Training Plan, a “Train the Trainer” program must be identified.

The Training Plan shall include at a minimum:

i) A description of all training courses including identification of the purpose and goals of each course, duration of the course, type of training (presentations, hands on training) and identification of the facility and training equipment provided by the Contractor (e.g., lecterns, overhead projectors, televisions, video cassette recorders, specific Revenue Control System hardware elements, etc.).
ii) A list of classroom instructors who shall conduct the training and a description of their skills, experience and qualifications.
iii) Individual course curricula, course materials, manuals, study guides and workbooks.
iv) Course critique and evaluation forms for students.
v) Post-training and or on-the-job technical reference guides.
vi) A detailed schedule for the delivery of all training courses.

After receipt of the Training Plan, the Authority will formally comment on its content. The Contractor shall make appropriate changes to the Training Plan and resubmit it for Authority review and approval.

b) Training Program

After approval of the Training Plan by written notification from the Port Authority, the Contractor shall conduct the specified training in a Train the Trainer manner. The training program shall be implemented through the use of formal classroom training to a selected group of people for each of the below categories and those people will be responsible for training the other system users. The curriculum shall be designed so that each group of trainees shall be trained in the full repertoire of system commands, which they may have to use in the course of performing their designated functions. Students shall be provided with complete sets of training materials and operating manuals during the training sessions, which they shall retain for use on the job at the completion of training. Formal training shall also include a comprehensive student testing program for determining that the intended training has been successfully imparted. The Contractor shall provide additional training and testing materials to be used in the subsequent training programs.

Scheduling of Train the Trainer instruction classes shall be coordinated by the Contractor and Port Authority personnel to avoid conflicts and peak-period personnel demands. The Contractor shall submit a proposed instruction schedule at a joint meeting conducted prior to equipment installation. The Port Authority shall tentatively approve or suggest changes to the Train the Trainer training schedule at that time. Forty-five (45) calendar days prior to each Train the Trainer instruction session, the Contractor shall submit to the Port Authority an outline of the instruction material and approximate duration of the session. Ample time shall be allotted within each session for the Contractor to fully describe and demonstrate all aspects of the PARCS, and allow Port Authority personnel to have hands-on experience with the PARCS.

There shall be two (2) separate types of training provided by the Contractor. Port Authority authorized personnel shall be trained via a Train the Trainer program in which the Contractor trains 20 personnel who in turn will train parking operations staff. All Train the Trainer personnel receiving training on the System shall be instructed in use of the system by Cashiers, Supervisors and LPR image reviewing personnel.

Separate trainings shall occur for both System Administrators and Accounting/Office Staff.

i) Cashiers

The Cashier training shall include the general operation of PARCS and LPR equipment at each airport, with each cashier Train the Trainer participating in two sessions.

(1) The first series of classes shall be conducted no later than ten (10) days prior to each facility's first scheduled Lane Acceptance Test date and shall consist of general system introduction and basic knowledge necessary to operate the system.
(2) The second series of classes shall be conducted shortly after each cashier has had experience with the PARCS and LPR Subsystem in an operational mode.

Initially, all cashier Train the Trainer personnel shall be instructed by the same personnel (unless otherwise approved, in writing by the Port Authority), and with the same processes.

A cashier's instruction terminal shall be provided to the Port Authority. This terminal shall be used during the instruction classes and left with the Port Authority for the instructing of future cashier staff.

ii) Supervisors

Supervisory Train the Trainer personnel shall be instructed in the operation of all components of the PARCS. The first series of classes shall be conducted in the two (2) weeks immediately prior to installation and activation of the New PARCS equipment and shall consist of a detailed system introduction and detailed knowledge necessary to operate the systems. The second session shall be conducted no more than thirty (30) days after each Supervisor has had experience with the new systems in an operational mode and shall include training on conducting minor repairs to field devices, up to but excluding board level repairs.

The instruction shall emphasize both hardware and software.

Initially, all supervisory Train the Trainer personnel shall be instructed by the same personnel (unless otherwise approved, in writing, by the Port Authority) and processes.

iii) Image Reviewers

Image reviewer training shall include the usage of image review software as part of the LPR Subsystem. The first series of classes shall be conducted in the two (2) weeks immediately before installation and activation of the New PARCS and shall consist of a general introduction to the image review software and basic knowledge necessary to use the software to review license plate images. The second session shall be conducted no later than thirty (30) days after each Image Reviewer has had experience with the image review software in an operational mode.

The length of each instruction class shall be defined in the Contractor's curriculum as approved by the Port Authority. Each instruction block shall be provided in a minimum of two classes, each covering the same material, and scheduled to ensure all personnel can attend one of the classes without undue disruption of normal work schedules.

iv) System Administrators

There will be approximately five (5) system administrators at each airport who shall be instructed in system administration, operations of all components, functions, and software.

The length of each instruction class shall be defined in the Contractor's curriculum as approved by the Port Authority. Each instruction block shall be provided in a minimum of two classes one which will be held during the day and the second class to be held in the evening, each covering the same material, and scheduled to ensure all personnel can attend one of the classes without undue disruption of normal work schedules.

v) Office Staff/Accounting

There will be approximately twenty (20) accountants, auditors and managers for each airport who shall be instructed in system operations, administration, reporting, audit and reconciliation procedure and software features. Instruction of the office staff/accounting/audit personnel shall commence in the two (2) weeks immediately before activation of the New PARCS and all its elements.

The length of each instruction class shall be defined in the Contractor's curriculum as approved by the Port Authority. Each instruction block shall be provided in a minimum of two classes, each covering the same material, and scheduled to ensure

all personnel can attend one of the classes without undue disruption of normal work schedules.

vi) General Training Requirements

The length of each instruction class shall be defined in the Contractor's curriculum as approved by the Port Authority. At a minimum, each class shall be two (2), four (4) hour training classes scheduled on two (2) separate days. Each instruction block shall be provided in a minimum of two (2) classes, each covering the same material, and scheduled at different times during the day, i.e. one class in the morning, afternoon or evening, to ensure all personnel can attend one of the classes without undue disruption of normal work schedules.

Maintenance staff shall be trained as factory certified maintenance technicians and shall be awarded certification upon successful completion of maintenance training.

All instruction courses shall consist of classroom instruction and actual "hands-on" experience. Classes shall be set up in a room designated by the Port Authority. The Contractor shall provide one (1) instructor for the duration of each program. The instructor shall speak fluent English in a clear and precise manner.

Class content shall be coordinated and developed with the Port Authority so that procedures for all transaction types are included. The class material shall include schematics, as well as an overview and descriptions of the equipment. The Port Authority reserves the right to videotape all training sessions for future instruction purposes or Contractor shall supply video demos if available.

The Contractor shall provide all documentation required for instructing Port Authority personnel. Documentation shall be provided for each student in the form of workbooks, lecture notes/overheads, and manuals for student markup. The Contractor-supplied instruction documentation shall be sufficiently detailed so that the user can in most cases resolve issues. The Port Authority retains the right to copy and print training materials as frequently as required for ongoing internal use only.

Any training that is in addition to the above will be paid for via the Work Order process. The above training will be included in the PARCS installation cost proposal.

At the completion of instruction courses, all Port Authority staff and contractor that completes the course shall receive a Certificate of Successful Completion.

vii) Training Materials

The Contractor shall provide the Training Manuals and any other associated course materials, study guides and workbooks, as described in the approved Training Plan. These manuals shall be for instructional use during the Training Program, for study and for refresher use to provide training of all the features and functions of the Revenue Control System during normal and emergency operations. These manuals shall also be for Authority or its contractors' use to train new operators, supervisors, system administrators and maintenance staff on an ongoing basis.

An instructional notebook or user's manual shall accompany every instruction course. The Contractor shall submit a hardcopy of the user's manual per the submittal guidelines. The Contractor shall supply twenty (20) bound, hardcopies of each user manual type: cashier, supervisory, image reviewer, system administrator, technician, audit and accounting, etc. In addition, all manuals (instruction and maintenance) shall be submitted in electronic format (.PDF) on a CD-ROM or DVD. Four copies of CD-ROM/DVDs shall be supplied. The user's manuals shall be written in common English with appropriate photos, diagrams, and schematics to supplement the text.

18) DISASTER RECOVERY SUPPORT

For the term of the contract, the Contractor shall be responsible for creating a Disaster Recovery Plan (DRP) for the Authority, testing the DRP on an annual basis, or in the event of a real disaster, participate in the DR recovery operation. This would include fail over / switch over to the secondary servers in the event of a primary production server failure. Such a fail over is expected to be done automatically and seamlessly as well as the fall back to the primary servers. Testing of this condition is to be done annually with Contractor support. Additionally the DRP would include establishing the System and related software components on an external Authority-selected alternate Disaster recovery site. The Contractor is expected to work with the Authority's Contract Manager to define the scope of annual disaster recovery tests, coordinate with other Authority staff and third parties to ensure all required tasks are covered and to conduct and evaluate the components of these Disaster Recovery tests. The Contractor shall be responsible for maintaining up-to-date Disaster Recovery plans, including projected and actual (based on Disaster Recovery tests) timelines for the various recovery steps. The Contractor is expected to do basic validation and ongoing tuning to ensure the resulting processes are always kept up-to-date and well documented. The Contractor shall test the DRP at least once a year at a minimum. The Contractor shall provide all documentation and all software, including third-party software to reconstitute the system.

Additionally, on a semi-annual basis, the Contractor shall be responsible for testing the backup media used by the Authority for the daily incremental and weekly full backup of the servers. The Contractor shall coordinate its work with the Authority's Technology Department to test the backup media.

19) BUSINESS RESUMPTION PLANNING

The Contractor shall work with the Authority to participate in activities associated with the Authority's Business Resumption Plan. The Contractor shall be primarily responsible for the portion of the plan concerned with providing continuing application management services for PARCS. The Contractor shall participate in any test of the Business Resumption Plan scheduled by the Authority, typically quarterly.

Parking Access and Revenue Control System—Design, Installation & Maintenance

Attachment E:
Functional Specifications

Attachment E: Functional Specifications

1. GENERAL NOTES

This Section contains the functional specifications and requirements for a new Parking Access and Revenue Control System (PARCS) to replace the existing one at the Port Authority of New York and New Jersey (the "Port Authority"). The PARCS Replacement includes Newark Liberty International Airport, LaGuardia International Airport, John F. Kennedy International Airport, and Stewart International Airport. The PARCS replacement shall not only utilize the industry's latest technological advancements to control access and calculate and accurately report revenue for the parking facilities but shall improve the overall management, system efficiency, revenue accounting, revenue security, customer service and marketing aspects of the parking operations at the Airport. This project shall implement hardware, networking and application software that shall meet or exceed the Port Authority's parking access and revenue control needs for at least ten (10) years after the system's final acceptance. These specifications shall describe the functional requirements for the New PARCS and what, if any, existing equipment may be used with the new system.

This project shall replace the existing parking access and revenue control system at all public and employee parking facilities. Some of the equipment for these facilities shall be identified as optional; therefore, Contractors shall provide separate pricing for all alternate proposal items as outlined in Attachment C2, Pricing Sheets. At minimum, a new system shall incorporate all of the functionality of the existing system.

A. REFERENCES

I. Codes and Regulations

a. Local Codes: Comply with State and Local codes as applicable.

II. Information Security Standards and Requirements

a. PCI DSS, latest version at the time of Contract Award
b. PA DSS latest version at the time of Contract Award
c. Latest version of EMV standards at the time of Contract Award

III. Port Authority Standards and Guidelines

a. The Technology Standards for the Port Authority (See Attachment K)
b. Guide to Systems Administration for Port Authority Technology (to be shared with Contractor upon commencement of the Contract.

c. Cyber Security Guidelines for the Port Authority of New York and New Jersey (See Attachment M)
d. Audit Controls Requirement Contract Checklist (See Attachment J)
e. Computing Resources Guidelines (See Attachment L)
f. ACH & ECH Interface Requirements (See Attachment T)
g. The Port Authority of New York and New Jersey Information Security Handbook (Attachment O)
h. The Port Authority of New York and New Jersey Cloud Computing Framework (See Attachment W)

B. DEFINITIONS

Automated Pay Station—a computerized PARCS device that facilitates payment of parking fees prior to a patron returning to his/her vehicle. Also referred to as a Pay-on-Foot Station, POF or Merli Machine.

AVI– Automated Vehicle Identification—An RFID that emits an electronic signal that can be read by an associated reader/antenna. The signal contains information relating to the account and transponder number.

Barrier Gate – An automated gate utilized by the PARCS to control ingress into and egress from a parking facility.

Cashier Station – a computerized PARCS device located in a staffed cashier booth at an exit lane that facilitates multiple methods of exit from a parking facility; also referred to as cashier terminal.

CBEMA – Computer and Business Equipment Manufacturers Association: The CBEMA curve illustrates the acceptable under-voltage and over-voltage conditions that most equipment can sustain for a period of time.

CCI/CCO – Credit Card In/Credit Card Out: an express parking transaction whereby a patron inserts a credit card into an entry station to gain access into a parking facility. Upon exit, the patron inserts the same credit card into the exit station. The system matches the entry event with the exit event, so as to positively identify the vehicle and patron, calculates the appropriate parking fee, and charges the credit card. Upon positive authorization of the credit card, the barrier gate raises and patron exits the facility.

Conceptual Design Document – This document, to be prepared by the selected Contractor and subsequent review meeting shall insure Contractor has a full and complete understanding of the Port Authority's parking operations and the requirements of this specification for the New PARCS.

Contract Documents – The Contract Documents, as set forth in the Award Letter, executed by the Port Authority and the Contractor outlining the requirements for the Work to be performed as it relates to the implementation and maintenance of the PARCS.

Contractor – The individual, partnership, firm, or corporation primarily liable for the acceptable performance of the Work contracted and for the payment of all legal debts pertaining to the work who acts directly or through lawful agents or employees to complete the work.

Critical Design Document – This document shall contain detailed description of the proposed PARCS and system components including schematics, diagrams, interface control documents, etc.

Customer Loyalty Program – A program to provide benefit to patrons who frequently park at the airport. This system shall be a web-based application to allow patrons to sign up and maintain their account. This system is tied to the vehicle license plate number or AVI account and shall recognize a vehicle with an approved account, open the exit gate and bill the credit card on file. Also referred to as a "Frequent Parker Program."

Dynamic Signage – signage displaying varying text and/or graphics to relay specific messages to patrons. It includes the following major components: sign face, sign housing, controller, and, if present, the controller cabinet. Dynamic signage can be used for various applications including displaying the method of payments accepted at a specific lane, the number of available spaces in a facility/level, or providing guidance to patrons. Also referred to as a DMS, VMS or CMS.

EMV – European MasterCard/VISA credit card standard, referring to a chip embedded credit card associated with a personal PIN used for payment of parking fee due. Sometimes referred to as "Chip and PIN".

Entry Station – a computerized PARCS device located in an entry lane that facilitates multiple methods of entry including issuing a magnetically encoded or barcoded parking ticket, ingesting and reading a magnetically encoded or barcoded access card or credit card, reading an EMV (chip embedded) card, reading an AVI transponder, reading a proximity access card, reading a bar code or QR code from a cell phone or hard copy document, or reading a contactless credit card; commonly referred to as: ticket issuing machine or TIM.

EWR – Newark Liberty International Airport

Exit Station – a computerized PARCS device located in an exit lane that facilitates multiple methods of exit from a parking facility including ingesting and reading a magnetically encoded or barcode parking ticket, ingesting and reading a magnetically encoded or barcode access card or credit card, reading an EMV (chip embedded) card, reading a bar code from a cell phone or hard copy document, or reading a proximity access card or credit card fob via RFID. The exit station uses the data from the inserted or detected media to validate exit privileges or calculate and process the associated parking fee; fees can be paid via credit card, debit card, or cell phone, or exit is granted via access card or validated/pre-paid magnetically encoded ticket; commonly referred to as: express exit terminal or exit verifier.

FAT – Factory Acceptance Test: a test of the PARCS Contractor's system and equipment prior to delivery to a project site to ensure that the equipment and system meets the intent of these Functional Specifications.

FMS – Facility Monitoring System: A system that provides operational and performance information of all system components.

Frequent Parker Program – A program to provide benefit to patrons who frequently park at the airport. This system shall be a web-based application to allow patrons to sign up and maintain their account. This system is tied to the vehicle license plate number or AVI account and shall recognize a vehicle with an approved account, open the exit gate and bill the credit card on file. Also referred to as a "Customer Loyalty Program."

GUI – Graphical User Interface: A program interface that takes advantage of a computer's graphics capabilities in an attempt to make the program user-friendly and intuitive to use.

IRW – Image Review Workstation: a workstation that is used to review images from the LPR system.

ISO –International Organization for Standardization: An international organization comprised of national standards bodies from around the world. ISO is the world's largest developer and publisher of standards.

JFK – John F. Kennedy International Airport

LAT – Lane Acceptance Test: a test of a Contractor's installed equipment at the lane level to ensure that the equipment meets the intent of these Functional Specifications. LATs are conducted on all entry lanes and exit lanes. LATs shall also need to be conducted for POF machines.

LED – Light Emitting Diode: a type of light commonly used for dynamic signage.

LGA – LaGuardia Airport

LPI—License Plate Inventory

LPN – License Plate Number

LPR – License Plate Recognition: May be one or a combination of cameras plus software, infrastructure, and monitoring stations that allow for the automated recording of a vehicle's license plate number upon entry and exit using application software utilizing OCR. The license plate number is linked to the vehicle's entry and exit traversals within the PARCS. Upon exit, the license plate is checked again by the PARCS to verify that the vehicle attempting to exit is the same vehicle that is linked with the entry traversal of that transaction; This may be incorporated into or be a subsystem to the PARCS.

NEC – National Electrical Code

OCR – Optical Character Recognition: a set of software algorithms that enable LPR application software to analyze a digital image of a license plate and determine the digitized values of the license plate characters through an automated process.

Open Architecture—a type of computer architecture or software architecture that is designed to make adding, upgrading and swapping components easy.

ODBC – Open Database Connectivity: In computing, ODBC provides a standard application software programming interface method for using database management systems. ODBC is intended to infer an independence from programming languages, database systems, and operating systems.

PA DSS – Payment Application Data Security Standard: a set of comprehensive data security requirements and parameters for computer applications that process credit card payments.

PANYNJ – The Port Authority of New York and New Jersey: the owner and initiator of this project. Also referred to as "the Port Authority" or "Authority" or "PA"

PARCS – Parking Access and Revenue Control System: A combination of equipment, subsystems, and supporting infrastructure including operational procedures, software, firmware, websites, documentation, etc. that allows an

entity to accurately calculate, collect, track, and report revenues for parking within one or more facilities. A PARCS also monitors and controls ingress and egress to and from those facilities as well as providing other functions, as outlined in this document. Also referred to as "System" or "Existing PARCS" or "Existing System" (for existing 3M PARCS) or "New PARCS" or "New System" (for System to be installed)

Pay-on-Foot Station—a computerized PARCS device that facilitates payment of parking fees prior to a patron returning to their vehicle. Also referred to as an Automated Pay Station, POF, APS or Merli Machine.

PCI DSS – Payment Card Industry Data Security Standard: a set of comprehensive requirements and parameters for enhancing payment card account data security to help facilitate the broad adoption of consistent data security measures on a global basis.

PIN – Personal Identification Number: A number selected by a user to gain access to certain areas of the PARCS or to associate with a chip embedded credit card required by EMV standards.

Preventive Maintenance - This type of maintenance includes but is not limited to scheduled inspection, testing, necessary adjustment, alignments, lubrication, parts cleaning, replacement of consumables, communication system maintenance, server administration, database administration, and application support of the PARCS hardware and software.

PSCS – Parking Space Count System—a combination of vehicle detection sensor devices, dynamic signage, and supporting infrastructure that allow for the automated counting of vehicular ingresses and egresses to and from a parking facility. The resultant count is displayed on operational workstations as well as a series of dynamic signs to inform patrons of the location of available parking; a subsystem to a PARCS.

QR Code – A QR code is a form of a bar code that can store more data than a standard binary bar code.

Remedial Maintenance- This type of maintenance is repair service that is required because a system component has malfunctioned.

RFID – Radio Frequency Identification: the technology utilized by proximity card systems or Automatic Vehicle Identification systems, such as *E-ZPass® Plus™*, HID™, or PayPass™, for identifying a patron's credential. A RFID system consists of an antenna, a transceiver (which reads the radio frequency and transfers the information to a processing device), and a transponder, also called a tag (which

is an integrated circuit containing the RF circuitry and information to be transmitted).

SNMP – Simple Network Management Protocol: SNMP forms part of the internet protocol suite and is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SQL – Structured Query Language: a database computer language designed for the retrieval and management of data in relational database management systems, database schema creation and modification, and database object access control management.

SWF – Stewart International Airport

System – See "PARCS"

TCP/IP – Transmission Control Protocol/Internet Protocol: The Internet Protocol Suite (commonly known as TCP/IP) is the set of communications protocols used for the Internet and other similar networks.

UPS – Uninterruptible Power Supply: A UPS is a device that maintains a continuous supply of electric power to connected equipment by supplying power from a separate source when utility power is not available; also known as a continuous power supply or a battery backup.

C. REQUIRED SYSTEM OBJECTIVES

The objectives of the PARCS project include, but are not limited to:

I. Build a New PARCS to replace the Existing PARCS.
II. The New PARCS shall be designed with an open architecture and adherence to industry standards in order to provide future integration to any third party applications and equipment.
III. Contractor shall reuse existing infrastructure when possible, including such items as existing conduit, AVI equipment, cashier booths, etc.
IV. Provide mechanisms to strengthen internal controls and minimize theft and loss of revenue.
V. Achieve a PCI PA DSS compliant environment and maintain the cardholder environment consistent with ongoing compliance.
VI. Provide flexibility in offering new capabilities to promote parking and other Port Authority services in a web-enabled environment including prebooking and prepayment capabilities.
VII. Accurately track required financial and statistical information.
VIII. Accurately calculate appropriate fees.

IX. Accurately document the revenues generated by the parking operations.
X. Increase efficiency of operations and maintenance through reduction of person-hours required for parking occupancy validation.
XI. Provide flexibility in the timing and formatting of the pertinent operational and management reports.
XII. Provide flexibility in rate configurations for all parker types, and to vary rates by time of day and day of week, special events, type of parker.
XIII. Provide a monthly parker program with both over the counter payments and corporate monthly payments, which can be selectively integrated with the Port Authority SAP accounting software for billing and reconciliation of monthly parkers. Provide granularity to individual vehicle levels for monthly parkers including non-revenue for Port Authority and selected vehicles.
XIV. Ensure flexibility and scalability for any future need to update, upgrade, and/or expand the system readily (additional lanes and parking products as well as additional facilities).
XV. Provide an intuitive and user-friendly interface for the Port Authority and other personnel.
XVI. Provide electronic coupons and/or validations that may be presented by the patron in all lanes, including processing in self-service lanes.
XVII. Provide business intelligence tools for better managing parking system and forecasting results of potential modifications or additions of programs.
XVIII. Provide Loyalty programs specified and designed by user, e.g. fee adjustments for frequent users, corporate program users.
XIX. Provide simplified maintenance procedures for lane and back-office equipment furnished by Contractor.
XX. Maintain Existing PARCS system in a state of repair to support current operations until a replacement system is fully installed and operational.
XXI. Maintain the New PARCS in a state of good repair to comply with the availability and reliability requirements herein.

D. Optional System Objectives

I. Accurately calculate parking space availability on a level-by-level, zone-by-zone and space-by-space basis, depending on the required granularity per parking facility.
II. Accurately calculate and disseminate parking space availability for the desired level of granularity to dynamic signage and existing parking information web sites and allow for future dissemination of information to mobile devices and web sites.

E. Additional Facilities

During the life of the New PARCS, the Port Authority may add facilities that shall provide additional public parking. The proposed New PARCS shall be

upgradeable, scalable, and modular in design such that it can support all of the future needs of these facilities. The system shall be designed with excess capacity so that growth can occur without any degradation in system performance even during peak periods. Transactional volumes at the four airports in 2015 were:

I. John F. Kennedy International Airport: 4,112,611 paid cars
II. LaGuardia Airport: 1,170,759 paid cars
III. Newark Liberty International Airport: 2,872,335 paid cars
IV. Stewart International Airport: 69,443 paid cars

F. Component System Integration

The parking and other control equipment components provided by the Contractor shall operate as a complete system. Each equipment component shall perform its function in relation to other components. As such, each component shall be compatible with all related components. All components shall be compatible with the geometric circumstances of the facility or place where they are installed.

G. Specification Discrepancies

The Contractor shall bring any omissions or discrepancies in these specifications that they believe may exist to the attention of the Port Authority in its Proposal. No deficiency or discrepancy in these Functional Specifications shall relieve the Contractor of the responsibility to provide a satisfactorily performing, reliable system.

H. Cashier Booths and FOICs (Fiber Optical Interface Cabinets)

The Contractor shall identify and supply to the Authority a list of cashier booths and FOIC's that cannot accommodate their equipment and that may need modification or replacement as part of the Submittals. The list shall include the item or items of each booth or cabinet which fails to meet their equipment needs.

I. After award of contract the Contractor shall perform a walk through at all airport parking facilities and identify the number of entry and exit lanes, entry and exit plazas, POFs, FOICs and communication nodes, server locations and operations locations.

2. SOFTWARE

Parking access and revenue control software for each airport shall run in a separate computing environment that has a diversely located backup and is dedicated to airport parking access and revenue control. The hardware for both the primary and backup computing environments will be provided and maintained by the Authority. See Attachment B "General Contract Terms and Conditions" for details on Net Cost Work. Subsequent to finalizing the Contractor's submitted server architecture and requirements, the Technology Department will build the servers in the Authority provided computing environment(s) in accordance with the Contractor's stated requirements and create a production and Quality Assurance test environment for the Contractor's use. The Contractor will be provided with remote access to the production and QA test environments to install, configure, test, make operational and administer its application software in the Authority provided servers. The QA test environment will to be open to authorized users, as determined by the Port Authority and Contractor needs.

A. The Port Authority will provide and install the operating system and database software on the requisite servers in accordance with the Contractor's requirements approved at a hands-on Technology workshop and in compliance with the Technology Standards for the Port Authority (see Attachment K), and purchase the software licenses for the operating systems and database software. The Port Authority will maintain and administer the operating system and database software and their software licenses and maintain their ongoing software support contracts. All other software and software licensing required to develop, maintain and make the applications software operational shall be provided and maintained by the Contractor.

B. The Contractor shall identify each software package it intends to use in its Proposal. Unless specified elsewhere, all third party software provided by the Contractor shall be the latest available version at the time of system implementation and the Contractor shall update the third party software with all released patches and critical updates, at no additional cost for the duration of the duration of the Contract. All third party software shall be licensed to the Port Authority.

C. Upon execution of the Contract, the Contractor shall provide perpetual licenses for all Contractor furnished and third party software used as part of the PARCS. This includes all operating system software approved by but not furnished by the Authority, application software, software used for application development and system generation, peripheral software, and PARCS hardware diagnostic software. Site licenses shall be provided to the Port Authority for each airport. The Contractor shall identify any and all third party software and their associated licenses and manufacturer's support services in the Proposal. The Contractor shall also provide software maintenance agreements for all third-party software for support, patches and future updates. The Contractor shall replace all third-

party software that is no longer maintained by the third party provider, in accordance with the net-cost provisions of the Contract. Original CD-ROMs, DVDs, and software documentation shall be delivered to the Port Authority prior to system acceptance testing. CD or data vaults may not be put on the servers and data may not be removed or inserted on the servers by the Contractor. The Port Authority shall provide Application Administrator staff to support data transfer at the request of the Contractor.

D. Time Control

I. The Central Computer shall include a Time Control function for time-initiated events and as a master clock for the entire system.
II. The system shall be able to synchronize all clocks from a central point automatically on a schedule to be set and modified by an authorized user (System Administrator). It shall also allow for sending the time under manual control to one, several or all devices as needed.
III. The system shall be able to compensate automatically for daylight savings time in the Spring and Fall.
IV. Validity checks are necessary to ensure that the master clock used to set the system time is not outside reasonable parameters as measured against the last reboot of the system or change to the current setting.
V. Access to the "Set Time" functions shall require a valid password.
VI. Any access to the function as well as modification to the current date and time shall be automatically reported for auditing and to the Event Log.
VII. Network Time Protocol and Time Synchronization
VIII. Applications that require time and date synchronization shall query PAWANET to obtain the current time of day and date using the network time protocol (NPT).

E. Database Management System

I. Application software shall consist of software to provide complete operation of the PARCS, including the database.
II. The Contractor shall select a database management system that complies with the Technology Standards for the Port Authority referenced in Attachment K.
III. The database management system (DBMS) hardware, software, licenses and software support contracts shall be furnished by the Authority. The installation, setup, configuration and administration of the DBMS shall be performed by the Authority in partnership with the Contractor.
IV. Data recorded by the PARCS shall be maintained in files that are in ODBC compatible format for the retention periods stated herein. Solution shall support a relational database format for the storage of data based on Port Authority standards.

V. The database shall be read available to authorized PA personnel or their designees.

VI. The application Administrators shall have access to all database logs and performance tools to monitor performance of database and system.

VII. The real time performance of transaction handling shall not be adversely impacted by the running of reports.

VIII. The Airport and system servers shall store all information for a minimum of thirteen (13) months in an appropriate database format, and such information shall be available for Authority use in a format accessible by standard database packages.

IX. The system shall store all data relating to the operation of the PARCS in relational databases. The Database Manager shall support standard SQL commands and queries and shall be capable of performing the necessary functions described herein. A single database shall be used for the storage of data throughout the PARCS.

X. Data older than thirteen months or no longer considered "active" data shall be automatically archived at a location to be identified and subsequently be readily available and easily accessed for retrieval, reporting and query purposes. Archiving procedures shall be established and documented by the Contractor. The database engine provided shall be SQL/OBDC compliant. The archival process shall not interfere with normal online operations.

F. Operating System Platform

The network and server operating system shall be furnished, installed, configured, maintained, and administered by the Port Authority. Based on the system architecture that will be jointly formulated during the Hands On meeting with the Technology Department, servers located in the public and private DMZ will be hardened to the Technology Department's standards.

G. Application Software

I. Application software shall be comprised of computer application programs to provide complete operation of the PARCS. The Contractor shall be responsible for making its application software compatible with the furnished operating system platform. The software programs provided shall allow for future upgrade and expansion of the PARCS in a timely fashion and without adversely interfering with existing functionality.

II. Servers and workstations solution shall allow multiple groups and roles that govern individual access to the system and transactions within the system. The assignment of a group/role shall determine whether or not the individual may access a functional area, subsystem, table, report or transaction, and if the access is update or view only. The User's Access privileges shall be

retrieved from the Authority's Active Directory as part of the user authentication process. The PARCS software shall provide the following:

a. Access to any function that could compromise the integrity of the operating system or application software shall be password controlled and shall comply with current, up-to-date PCI standards and the Technology Standards for the Port Authority (see Attachment K). Separate login shall be required for the separation of file maintenance and routine data entry and retrieval.
b. The most up to date PCI Compliance standards, at the time of proposal.
c. The PARCS software shall provide a login and privilege capabilities which shall integrate with Port Authority active directory but not be dependent on it should network access be compromised. Login and Logout at the Cashier stations shall also be available locally with the ability to sync up with the servers when communications are restored.
d. All changes to data, system, financial transactions or system shall be logged and recorded in accordance with PCI requirements. No change shall jeopardize PCI Compliance.
e. Application software Logging and Alert Notification
   The System shall provide complete logging for the following types of System activity:
   1) User Activity Log – This feature shall record all log in and log out activity by user, name and IP address of device used to log into/out of the system, time and date and shall record event descriptions for each, including changes made to the System setup or configuration, retaining both before and after values. The system shall also log all unsuccessful attempts to log into the system, recording the user name used, name and IP address of device used to attempt to log in the system and the time and date the attempt was made.
   2) System Activity Log – This feature shall record all events in the System. It shall include the user name, type of activity, time and date, requested changes and impacted equipment.
   3) Fault Log – This feature shall log all System faults. It shall include type and location of fault, time and date of fault, time and date of restoration, impacted equipment and any applicable information related to the repair.
   4) The System shall issue an alert and send an email to notify the operators of any observed faults or system failures. The capability shall be to allow the System to issue a separate alert to a different email address for each of the different fault conditions that can occur.

   Since the event logs can grow over time and consume a great deal of space in the database, the System shall archive log entries older than a

user-specified number of days from the PARCS revenue Database and archive the entries to an Archive Database in order to maintain system performance. The archive process will be performed during a time when system activity was very low, i.e. 2:45 AM, to ensure minimal impact on the performance of the PARCS application. The archive database would be physically separate from the operational database, i.e. physically located on another server, in order to minimize any impact on the performance of the PARCS application when querying the event logs. The Contractor shall create a set of Authority-approved reports to enable users to query both the application and Archive Databases, filter the log entries based on a date range, action, user, message type and record identifier, and report on the results.

The Archive Database is a database instance that is separate from the online PARCS database containing revenue data.

f. Browser-based – PARCS software shall be browser-based and web enabled, i.e. the PARCS software shall be accessible by an authorized user through an internet browser that complies with the Technology Standards for the Port Authority (see Attachment K). Users shall not need a client version of the software installed on their workstations to access the software. The Contractor will identify if application and system administrators need client access in the performance of their duties. Access rights to the system for all classes of users from any source shall be defined during implementation.
g. Software shall provide role-based access control using the principle of least privilege for all system functions including system administration and security administration. Access privileges shall be constrained to the minimum amount of privileges that will allow users to perform their duties based on their documented roles and responsibilities.
h. Active Directory Aware
The application software shall be Active Directory Aware and fully integrate with the Port Authority's Active Directory infrastructure for user authentication and access privileges. The Contractor shall coordinate its work with the Port Authority's Technology Department to integrate its application with the Port Authority's Active Directory infrastructure.
i. All Workstations and Lane POS units shall incorporate a locked screen saver functionality with the exception of POFs and any lane without a keyboard or screen. The time interval shall be modifiable only by authorized Authority personnel.
j. Integration with the Port Authority's website – The PARCS shall utilize web services to push data from the PARCS in real-time, and/or timed intervals or time-of-day, in a format specified by the Port Authority, to be published on the Port Authority's website. The PARCS shall be able to

push data to other websites from time to time in the same fashion as to the Authority's website. The PARCS shall also be able to accept data from the Authority's Web servers or approved third party vendor sites. The Port Authority shall construct the website page(s) and inform the Contractor of the specific information to be published. At a minimum, the integration shall accommodate:

1) Real-time Open/Full percent capacity filled status and graphical depiction of each public parking facility – homepage, mobile website, or mobile application.
2) The real-time number of available parking spaces in each public parking facility – homepage, mobile website, or mobile application
3) Current rate structure for each parking lot.
4) Hyperlinks for access to Loyalty program registration and access to user accounts.
5) Marketing messages and integrate with other Port Authority marketing programs.

k. The system shall be able to charge variable rates based upon the time of day, day of week, and special events. The Contractor shall provide independent, variable rate structure for each Facility. The system shall account for daylight savings time changes when using variable rates.
   1) The rate structure shall be programmable to establish hourly, daily, weekly, monthly maximum fees, grace times, and complimentary periods.
l. Automatically detect and report fault conditions through a FMS - The system shall perform a self-check on a routine basis and provide notification for fault conditions and equipment failure. Fault conditions shall be categorized by severity and the system shall notify designated personnel via email and text message for any individual fault condition, category of fault, or Port Authority-selected group of faults. The System shall have the capability to issue a unique alert to one or more specified email address(es) for each category of fault. The system shall provide a continuous end-to-end self-check.
m. Reporting in accordance with requirements.
n. Allow Port Authority authorized Supervisors to authorize exception transactions occurring in any exit lane remotely or locally from a workstation in the parking office. Authorization shall be auditable by supervisor name, action taken, date, and time. The PARCS shall provide a "drop down" box to facilitate authorization of common exception transaction processing descriptions/explanations. All other exception transactions shall require a more definitive explanation to be entered by the Supervisor prior to the completion of the transaction.
o. Require Supervisors to enter reason for their adjusting the fee by any approved means (dollars, time in lot, etc.) for any ticket in a comment

field. Each use of this function shall be automatically logged in the system with date, Supervisor name, action taken, date, and time.

p. Central access and control of field devices – Users with the appropriate authorization shall have the ability to issue remote commands from system workstations to the field devices such as raising and lowering the barrier gates; rebooting the entry or exit station; putting the entry or exit station in or out of service; changing the lanes status signs; applying software patches and updates; etc. The use of central controls shall be logged with appropriate information such as: user ID, time, device controlled and action taken.

q. Parking rate, grace period, and time increment changes – All parking rate, grace period and time increment changes shall be conducted at the server level and shall be auditable within the system.

r. The PARCS shall remotely communicate with all devices in real-time for a general broadcast of information or software updates or to communicate to a single or subset of devices to upload such information or software. Broadcasting information such as rate changes or time increment changes shall be in real-time to all field devices. It shall be possible to remotely suspend or shutdown a field device's application or operating system, upload updates and remotely restart the application field device. Where the update does not impact current in-process transaction processing, it shall correctly process parking fees during a transition:

s. System generated alarms – System shall generate alarms for any user selectable event type. Alarm Hierarchy shall be completely configurable so that the Port Authority can adjust priority of alarms, audible tones, where the alarms are sent (email, text, etc.), etc. Initial Alarm Hierarchy shall be coordinated with the Port Authority during implementation. Selected alarms shall stay visible and shall require Supervisor response to be satisfied. The Contractor will provide a list of all events that can be alarmed for the Authority to review.

t. Ability to export all query results in multiple formats including comma-separated-value, Microsoft Excel©, Microsoft Access©, XML, etc.

III. Industry standard software packages can be utilized. Each such software package shall be identified in the Contractor's Proposal. The Contractor's Proposal shall state the purpose of the software package, where it shall be used, and how it shall be used. If one software package is required to interface with another software package, the interface shall be documented and supported by flowcharts or block diagrams as appropriate. The Contractor shall advise if the software used in the system shall be customized or "off the shelf" software, and shall describe the method of obtaining further software updates or modifications. Application software shall have been designed for use in PARCS and Parking Space Count System (PSCS) systems, and shall be written in a standard, industry-accepted computer language such as Java, C++, Visual Basic, etc. The Contractor shall identify the

version of PARCS and PSCS software that shall be used at the Port Authority in their Proposal. On-going maintenance costs, including licenses and/or fees for such packages must be provided.

H. Rate Control

I. A critical portion of the system is the ability to provide a flexible and comprehensive rate structure with the ability to report on the results of such a structure in detail and by a variety of summarizations. The patron fee shall be computed locally at:
   a. exit lanes (Cashier Terminals)
   b. Pay On Foot machines (POF)
   c. Point of Sale (POS) applications such as a Reservation System and mobile payment system.

II. This includes all normal and non-revenue fees when applicable (Non Revenue does not apply at a POF). The system shall be able to distribute the rate information from a central source to the individual POS units (CT, POF, etc.) either individually or in selectable groups or entirely.

III. For each lot or garage, a different "rate code" shall be encoded on the entry identifier (i.e. ticket) by the entry lane equipment designating the rates in effect at the time of entry.

IV. The number of rate codes shall be unlimited and may differ for each airport and type of lot (i.e. hourly, daily, etc.).

V. The system shall prevent a patron from leaving a lot or garage if the rate code on their identifier is not supported by the rate codes active at the exit terminal.

VI. In calculating the fee, there are four (4) different adjustment time factors which shall be taken into account. (These factors are part of the rate structure):
   a. The Grace period: the grace period is given at the POF after a payment to allow the patron time to get the vehicle to the exit. This is to allow a patron time to reach their vehicle and depart. This may vary by lot or garage.
   b. The Complimentary period: the complimentary time period is the maximum elapsed time between entry and exit for no charge. This shall be configurable by lot or garage. Normally applied for the entire airport but can be set for a lot.
   c. The Traffic Adjust time: the traffic adjust time is used at a Cashier Terminal to avoid penalizing patrons during a long queue period. The parking duration shall be reduced accordingly for fee calculation. The time periods shall be configurable by lot and lane. Only authorized personnel can make the adjustment.
   d. Snow Emergency adjustment time: The period of time declared by the airport for snow emergency conditions where vehicles could not exit the

lot. This shall reduce the parking duration in a similar fashion as the Traffic Adjust time and can only be initiated by Port Authority personnel.

VII. Handicapped persons shall obtain the lowest rate in the airport (normally the long-term rate).

VIII. The system shall allow authorized users to:
   a. Modify the various rates.
   b. Change the duration of the grace periods.
   c. Update the rate structure in effect at a POF, an application, a lane, a lot or for the entire airport from a central source.
   d. Modify the Traffic Adjust and/or Snow Emergency times.
   e. Modify the Complimentary time.

IX. The rate structure shall accommodate new and old rates, the dates they are to go into effect, and appropriate fee calculations for those patrons parked during a rate change.

X. The rate in effect on entry shall be the rate to be applied on exit regardless of the number of rate table changes between the two times. An unlimited number of rate table changes to be applied shall be provided.

XI. An authorized operator shall be able to update or modify any rate of the Rate Control System with proper permission from a workstation. The downloading of new rate parameters shall be separate from the updating of said parameters.

XII. The system shall maintain a detailed audit trail of all data related to rate changes, rate updates and distributions.

I. Fee Calculations

I. Fee calculations shall be based on the exit date/time less the entry date/time and are to take into consideration the grace periods, Complimentary time, manually entered adjustment times, Traffic and Snow Emergency adjustment times. This value cannot be less than zero (0).

II. The system shall maintain a detailed audit trail of all data related to the fee calculation.

III. In the event of a lost or mutilated ticket, the system shall:
   a. Check the LPR tables for a matching entry based on the LPR and image of the vehicle in the exit lane. The system shall display the two (2) closest entry images found in the system to the cashier and make available other possible matches when requested by the cashier. The system shall search for LPR information from the entry lanes in the same lot as the exit lane with the ability to search other specific lots based on a configuration setting.
   b. If no possible entry LPR match found, the system shall check the License Plate Inventory for a match and perform the fee calculation based on the information found in the record for a lost ticket. The current day shall be considered a full day for these purposes.

c. For a mutilated ticket the system shall allow the cashier to manually enter the printed information on the ticket into the cashier terminal

IV. Multiple Exit Grace Periods should be included in each rate table. POFs and mobile devices shall be able to have different Exit Grace Periods.

J. Audit Reporting

I. The Contractor shall review all existing reports and prepare a cross reference as to which of their Standard Reports would replace the current ones in use and what changes, if any, would be required to provide missing information.

II. The PARCS system shall document parking revenue and activity and generate revenue and activity reports. All reports shall be available online, report data from user-specified dates, and on demand for Port Authority personnel who have proper password access.

III. The Port Authority shall establish its virtual midnight for transaction processing, credit card batch close, and report cutoff times separately for each airport. The establishment of virtual midnight shall be a Port Authority responsibility that follows applicable instruction and training of Port Authority personnel by the Contractor.

IV. The system shall identify and produce reports that can reflect separately public parking, and employee parking activities.

V. All parking data needs to be separated by Parking Facility, lane, POF, and Parking Product for reporting purposes.

VI. Provide electronic event journal that can be accessed by a Supervisor from a PARCS workstation during a cashier shift and following shift close to perform cashier closeout. The journal created for each POS shall at the end of each logical day be sent to server for review. For reporting and research purposes filtering shall be available for all data fields. The journal shall not replace the standard logging performed on servers, workstations and field equipment.

VII. A shift close report shall be automatically generated and made available at the control center when a Cashier closes a shift.

VIII. The PARCS transactional stream of data shall be compiled in an ODBC compliant database. The Port Authority shall prepare custom reports using this data including the exportation of data to a report generation application such as a Business Intelligence tool or Microsoft Excel©, or as a PDF file.

IX. All reports shall query, filter, and sort transactions by any associated data field.

X. Capture, record and report separately all exception transactions (reasons for eliminating tickets) such as (swapped, unreadable, lost, foreign, mutilated, used, disputed fee, cancelled, credit card transactions processed in an off-line mode, as a minimum). The complete list of exception transactions shall be agreed upon by the Port Authority during the design process.

XI. A reconciliation report of all tickets in vs tickets out, including exception is required. Any missing ticket numbers are to be identified and listed for review.

XII. Provide a listing and samples of the Contractor's PARCS standard reports including report descriptions, selectable data fields, and report layouts for Port Authority review and approval.

XIII. The Open visits report, including Credit Card In/Credit Card Out transactions, shall be used by the Port Authority or its operator with the appropriate rights and privileges to research and close such visits.

XIV. Contractor shall provide a definitions key for every report including a narrative description of what data each column and row represents and calculation formulas that define how all figures are obtained.

XV. The Contractor shall be required to modify or develop and prepare "custom" reports up to the end of the warranty period at no additional charge to the Authority. Beyond the warranty period the Contractor shall prepare additional reports in response to the Authority's work order request, reimbursed in accordance with the work order provisions of the Contract. The content and layout of the information in these new reports shall be dictated by the Port Authority in consultation with the Contractor.

XVI. The PARCS reporting subsystem shall be an embedded software component of the PARCS application.

XVII. The PARCS reporting subsystem shall be queried within the PARCS application to allow Port Authority staff to develop ad hoc reports. The system shall be capable of saving an unlimited number of ad hoc reports developed by Port Authority staff in addition to standard and custom reports developed by the Contractor. The Contractor will provide a naming scheme to differentiate Contractor supplied and PA ad hoc reports. All reports shall be viewable to authorized personnel via a browser. Sorting and Filtering by report categories, names, numbers shall be provided.

K. Reports

Reports constitute a major component of the Parking Access and Revenue Control System. The main purposes of the Reports in the PARCS is to capture the desired data based on the user-defined parameters and eventually present the same in a user-friendly manner.

I. General

a. Both consolidated and Airport-specific reporting requirements, including an enhanced level of automation to minimize manual system interaction and data entry is required.
b. The system software package shall include the necessary commercially available, standard third-party report generator (ex. Crystal Reports) and

associated tools to define, format and generate customized reports, customized queries, and integrate with other commonly used software packages as required. Alternately, the software package shall be integrated into the PARCS. All data shall be stored in a format that complies with the ODBC standard such that data may be exchanged as necessary with other similarly compliant applications. The Contractor shall utilize the Relational Database Management System to configure all database tables, relationships, queries, reports, forms and automated data procedures.

c. All reports shall be available both on screen and in printed format.
d. All reports shall be exportable in (XLS), CSV, or PDF formats.
e. The reporting system shall be able to incorporate data from external sources in formats such as spreadsheet or comma delimited CSV, into selected reports. The Contractor shall identify what formats are acceptable and the means for incorporating the data in its Proposal.
f. All detailed, transactional reports shall have totals that match to the totals in summary reports.
g. Reports shall incorporate an option for including archived data (data older than 13 months) in addition to the online data.

II. Reporting Software

The software shall provide the Authority with the capability to query the database to produce a series of reports for such areas as auditing, cash and ticket control, occupancy and rate management information. The structure of the data shall be such that the Authority can access the data files with programs or queries to produce its own reports, in addition to those provided by the Contractor. All stored data shall be available for such reporting. There shall be no limit to the number of such custom reports that can be stored in the database.

III. Query, Report, and Database Input Forms

a. Predefined input forms for all information to be entered by users shall be provided. These input forms shall be displayed on the workstation screens and provide “fill-in-the-blank” simplicity of use. Each blank on the input form shall correspond to a field in the associated database or a calculation.
b. Each query and report shall have an input form to enter data necessary to perform the task. Each input form shall be customized to the task being performed, and all shall follow similar layout and design themes. Input forms shall provide the following features and capabilities.
c. As necessary, the input forms shall prevent the user from completing the task until all required fields have been populated.

d. Where possible, input forms shall restrict entries to valid values.
e. All configuration data and operational parameters shall be populated and edited using input forms.
f. The input forms for queries and reports shall allow the user to select gradually more specific information by the use of pull-down menus.
g. Using input forms, it shall be possible for a workstation user to select all PARCS equipment (the default), all PARCS at any location, all PARCS of one type at any location, and any individual item of PARCS equipment for any query or report where equipment selection is relevant.
h. Using input forms it shall be possible for a workstation user to select all events (the default), all events of a given category, all events of a specified priority, and any individual event type for any query or report where event selection is relevant.
i. Where selections are restricted to valid values, the first value in the top menu layer shall be the default value for that selection.
j. Where possible, the pull-down menus shall be constructed from configuration database information, such as equipment numbers and locations, event descriptions and categories, transaction types, employee identification, etc. Pull-down menus utilizing configuration database information shall be automatically updated whenever the configuration data is changed by the Authority.
k. All input forms for reports or queries that review historical data shall include the ability to filter data for all fields. For example, it shall be possible to select data pertaining to all days (the default), all weekdays (Monday through Friday), all weekend days (Saturday and Sunday), and any single day of the week and by time of day ranges.
l. Where input forms require manually entered information, such as date and time ranges, the input forms shall utilize error checking to insure that data entry is correct.
m. When an input form is used to create a query or report, all fields to be populated shall be candidates for sorting keys. Each query or report input form shall provide for a minimum of three (3) fields to be selected as sorting keys, and each sorting key shall be configurable to sort in ascending or descending order. Default sorting keys shall be defined for each input form where used.

IV. Filtering

Generic filtering function shall provide an authorized user to select the criteria in one or more fields for data inclusion in a report. Filtering shall allow for single items or ranges and permit wildcards for online and offline report generation.

V. Query and Report Output Format

a. To the greatest extent possible, the output format of all queries and reports shall be of similar style. Each report and query shall produce data in tabular format with each column clearly titled on each page. Each row of output data (excluding column titles) shall be consecutively numbered. All reports shall include a cover page that provides the following information:

   1) Title of the report
   2) Date and time report was generated
   3) User requesting the report
   4) Complete list of input parameters and sorting keys used to create the report

b. Every page of all reports and queries shall include a header that indicates the title of the report, a one-line synopsis of key input parameters (such as TIMs, POFs, CTs, event category, duress alarms, etc.), the beginning and ending date and time (where appropriate), the date and time the report was created, and the page number of the report and the facility name.
c. The results of all queries and reports shall be selectable by the user to be available on the user's workstation monitor or printer. When results are displayed on the workstation monitor, it shall be possible to quickly scroll through the output by line and by page, to move to the first and last page, and to select a specific page number for display and printing.
d. It shall also be possible for the user to select query and report output in a form that is exportable to other applications, such as spreadsheets and graphical report presentations programs.
e. The general query and report output format, including the data export formats, shall be subject to the Authority review and approval at the Preliminary Design Review stage.

L. General Design and Performance Requirements

I. General Design Requirements

The Contractor shall, at a minimum, conform to the latest revision of the Technology Standards for the Port Authority (Attachment K) and industry best practices. The Contractor shall build the PARCS to comply with the most current version of the Port Authority's Audit Department's Control Guidelines (Attachment J) included herein and satisfy the checklists therein.

All services provided by the Contractor that are hosted externally to Port Authority IT infrastructure, including but not limited to software as a service, on-demand software, cloud computing, etc, shall comply with the

requirements and controls stated in the attached Cloud Computing Framework (see Attachment W). If externally hosted services are proposed for use, the prospective bidder shall submit documentation that demonstrate4s compliance with the Cloud Computing Framework requirements and control mechanisms in its proposal.

In the event of a conflict, between the requirements and standards, the more stringent criteria shall govern unless a waiver is explicitly granted in writing by the Chief Technology Officer.

a. Start Up

The System shall automatically execute all site-specific configuration parameters required to start up and enter the operational mode of the application software upon system initialization.

b. State of Common Usage

Software, database and communications protocols shall be in a "state of common usage," or industry-standard, and shall be an open architecture. Computer software shall consist of all system, application, and utility software required to meet the requirements of this Agreement. All off-the-shelf software shall be industry standard. The Contractor shall submit the latest commercially-available release/version of all software products in general use prior to System acceptance.

c. Shutdown

The System shall be capable of being shutdown in an orderly fashion and in a fashion that causes no anomalies in other subsystem components or software applications and no loss of data. Other subsystem components shall report no multiple errors nor be unavailable as a result of shutdown.

Upon shutdown, the System shall automatically notify connected workstations that system shutdown is imminent.

Only authorized users shall have the capability of shutting down the System.

II. General System Performance Requirements

a. The System shall consist of readily available, proven hardware and software elements, which are fully consistent with the System's design and operation as specified. It shall have the throughput, capacity, and

availability, as specified herein, to provide the required functionality. It shall meet the performance requirements identified herein and under the maximum loading when all System devices are engaged and performing their specified functions, with no loss of data or user control.

At a minimum, 90% of the time, the System shall:

1) Process exit transactions within 20 seconds of detection of departing vehicles or insertion of entry ticket at exit lane
2) Update patron fee displays within 30 seconds of detection of departing vehicles or insertion of entry ticket at exit lane
3) Use a maximum of 50% of internal memory and disk storage in the servers and workstations.
4) Use a maximum of 50% loading on individual processors under worst case loading when all devices are engaged and all System elements are in operation.

b. Graphical User Interface

A user-friendly graphical user interface (GUI) shall be furnished that is ergonomically designed to facilitate user operation in an intuitive manner and to minimize operator actions for information retrieval and system operation. The user shall be able to invoke any action or command with no more than three (3) mouse clicks and any additional required data.

The user interface shall be designed with streamlined business display screens to facilitate easy data entry and general viewing. Navigation tools/menus/keys shall be prominently displayed and provide consistent, easy movement within and between screens.

All control and reporting features shall have a logical hierarchical arrangement to engage the user through such features as pull-down menus, interactive graphics, dialog boxes, touch screens or other user-friendly means. The user interface shall prompt the operator with instructions or for additional information when user entry is required. The user interface shall not require the operator to memorize command sequences to perform operator controls. Context sensitive help or another form of on-line documentation for all functions and operations shall be provided.

All screen layouts shall be submitted for approval by the Contract Manager. The Contractor may request in writing for the Authority to provide any drawings or graphics of the project area reasonably required for use in developing system graphics. The outputs of such queries or

reports shall be sent to user defined disks locations and/or email addresses. The Authority shall identify where for each report or query.

3. POWER

A. Existing power infrastructure (transformers, panels, conduits, and cabling) shall be re-used by the Contractor to support the new PARCS and PSCS.
B. A lane specific UPS shall be installed within each lane (with the possible exception of employee lots) to provide full operation, for sixty (60) minutes at a minimum, to either restore failed electrical service or allow for properly shutting down the lane equipment. Existing UPS units in good repair that meet Contractor requirements shall be used with new system.
C. Existing cables may not be reusable where cables have become damaged or corroded. For this unforeseeable situation, the Contractor will be paid via the Net Cost provisions of the Contract. Contractor shall use its own staff or a Port Authority approved subcontractor for all cabling requirements. Port Authority shall provide contact information upon request.
D. The Contractor shall provide power grounding of all devices per NEC. If an isolated ground is required, there may be instances where power-conditioning equipment may be required due to the location of equipment in relation to the power distribution panel and transformers.

4. COMMUNICATIONS

A. The PARCS shall reside on an existing fiber optic cable communication backbone. Fiber optic communication shall be made available by the Port Authority at all entry plazas, exit plazas and POF cluster location and shall be utilized by the Contractor.
B. The Contractor shall select specific interfaces for lane equipment, however; standard, open-architecture interfaces at the physical layer shall be utilized. Ethernet shall be utilized from the computerized Lane Controllers to the Servers. The Port Authority will provide Ethernet connectivity, as required, to all Plaza and server locations.
C. All Ethernet equipment and design shall meet the Technology Standards for the Port Authority (see Attachment K).
D. Network switches shall be provided at each entry plaza, exit plaza, and pay on foot station by the Port Authority. Network hardware shall be provided, installed and maintained by the Port Authority.
E. The Contractor shall present its description and specifications related to Communications for approval by the Port Authority. The Contractor shall provide any additional electronic equipment (i.e. terminal servers, not network equipment) and cabling required to establish connectivity between PARCS hardware and Port Authority network hardware. Cat-6a cabling or better shall be used for all connections of less than 100 meters. Singlemode fiber optic cabling

shall be used for all connections in excess of 100 meters. Contractor shall conform to the IP and VLAN scheme provided by the Port Authority.

F. The Contractor shall provide the Port Authority with design requirements for port density and bandwidth at each network connectivity location as part of the design process.

5. EQUIPMENT AND SUBSYSTEMS

A. System Architecture

I. As part of its proposal, the Contractor shall propose a fault tolerant, redundant server architecture. Servers shall be provided, installed, and maintained by the Port Authority. The servers and accompanying hardware shall be housed in Port Authority facilities.

II. The Contractor shall design the PARCS to use separate primary and backup applications software for each airport. A separate primary and backup application software shall be used for the central management system.

III. The PARCS central software for each airport shall operate with full failover transition between the primary and secondary server environments at all levels.

IV. PARCS lane components shall be able to operate in a stand-alone condition (without server connectivity) for a minimum of twenty-eight (28) consecutive days without loss of transaction data. Should the minimum time-frame be exceeded, the Contractor shall provide a mechanism to manually extract all transactional data from the entry and exit lanes for upload to the servers.

V. Once the production environment is ready for operational usage, the Authority shall provide all of the servers necessary for the development/testing/training environment for testing of software updates done by either the Contractor or the Authority. A separate testing environment shall be provided, installed and maintained by the Port Authority and isolated from all facility production systems. The Contractor will include these units in its maintenance plan. Communications to the Test Bed identified in item 6 below will be provided.

VI. The Contractor shall construct a Test Bed on Port Authority property at an approved location that includes at least one (1) of every type of PARCS device at a minimum. Items such as loops may be substituted with alternative devices to simulate vehicle traversals in a lane.

VII. The PARCS shall be an open-architecture system where all interfaces (hardware and software) conform to national and ISO standards. Where there are no standards, documentation shall be supplied to the level defined by Open Architecture.

VIII. PARCS Network Management and Remote Monitoring

a. The PARCS shall be designed to support stand-alone operations at each lane (distributed system with intelligent devices) as well as centralized management of the PARCS.
b. The Intercom system, CCTV monitors, and printers, etc., shall reside in the Parking Command Center and selectively at the PARCS Operations Manager's office for each individual airport. The Port Authority shall provide the hardware for each Parking Command Center and connectivity between each Parking Command Center and the central servers.
c. The PARCS Servers shall contain all PARCS software databases that are associated with revenue-closeout activity statistics and designated reports.
d. Workstations shall be available for the operators, audit and control staff as well as the Authority operations personnel. These shall be supplied by the Authority. Access to the system shall be browser based for such staff. Any client based software needed on a workstation for systems activity needs to be identified and approved by the Port Authority before it can be installed by the Contractor. The Contractor shall need to maintain their application and to ensure it continues uninterrupted when the Authority updates the workstations.

IX. Maintainability

a. All equipment provided under this Contract shall meet maintainability requirements as follows:

    1) Incorporate features that shall reduce to a minimum the maintenance requirements for preventive maintenance, failure repairs, and performance verification, which includes the use of SNMP as described in the Technology Standards for the Port Authority referenced in Attachment K.
    2) Provide for the easy removal and replacement of component parts. Where fault tolerance is provided, hot swap out shall be supported.
    3) Design equipment for easy access, minimizing the removal of other items to gain access to a specific part.
    4) Reduce or minimize the requirement for specialized tools and test equipment.
    5) Design equipment so that performance can be verified, failures detected, and adjustments made with a minimum effort.
    6) All devices shall have electrical surge protection (comply with UL 1449).
b. The Contractor shall build into the system structured exception handling so that the system responds predictably to error conditions, without lock-up or "crashing," and without distribution of corrupted data throughout the system. Error handling includes those caused by hardware failures,

and errors caused by operators and errors induced deliberately or accidentally in software.

c. The Port Authority shall provide, install, and maintain anti-virus software on all server and workstation hardware, and maintain intrusion detection on all servers (See Technology Standards for the Port Authority for the complete list of all mandatory software). The Contractor shall confirm that all such protections are updated to the latest releases and report any discrepancies.
d. At the time of proposal, the Contractor shall notify the Authority of all test equipment necessary to support the PARCS.
e. The field intelligent devices shall be PC based with the latest processors available at the time of contract award and shall have sufficient memory capacity to retain a minimum of twenty eight (28) consecutive days of transactions plus minimum 30% built-in spare including buffer memory. A mechanism to manually extract queued transactions in a field device for on-site uploading to the servers shall be provided. The process to extract the data shall be rapid and secure. The process to upload the data to the server shall not cause performance degradation to the system as a whole and shall be able to upload and have processed 500 transactions an hour.
f. During implementation and testing, and for on-going support, remote access between the PARCS Servers and the Contractor's software support team for supporting and maintaining the system shall be provided in accordance with the most current PCI published requirements and the Technology Standards for the Port Authority (referenced in Attachment K).

X. System Hardware

a. All system hardware furnished by the Contractor shall be configured to maintain logs of all actions at the device whether such actions are done locally, remotely, or automatically by the system.

b. Network Hardware

1) Fiber optic network switches shall be provided by the Port Authority for aggregation of communications at each entry plaza, exit plaza, and POF station installed at FOICs and backbone nodes.
2) The Contractor shall request the Authority install any additional network switches that are required by the PARCS application to connect field equipment to the network.

c. Backup Server

1) The Contractor shall propose and provide requirements to the Port Authority (in accordance with the Standards and Guidelines for Port Authority Technology) for a host standby server solution that provides high availability and redundant data storage. All operational functions shall occur without data loss upon failure of any single memory or associated interface.
2) The Contractor shall propose a server architecture with no single point of failure that complies with the Technology Standards for the Port Authority referenced in Attachment K.

d. The Contractor shall propose storage capacity and performance requirements that meet or exceed the following:

1) Maintain thirteen (13) months of ALL data including but not limited to, transactional data, traversal data, log files and redo logs, maintenance logs, security logs, etc. This data shall be readily accessible on the real-time Server database, and should be accessible without any delay in processing.
2) Beyond (13) months: Keep operational data on-line for the prior seven (7) years, and year to date for the current year, cumulative to ten (10) years of data. The exception information shall be easily retrievable and software provided to assist an operator in building and maintaining a report/database of incidents. The Server's hard disk capacity shall be sized to process the transaction activities of the PARCS as described in these Performance Specifications as well as capacity for doubling the number of transactions and the operation.
3) Long Term Storage Media – The Servers shall have long term storage to archive the entire database for up to ten (10) years with simple retrieval. The Contractor shall provide a backup/archiving approach whereby reports are properly catalogued such that historical data can be retrieved, added to new reports, or printed. The Contractor will provide capacity requirements to the Port Authority, which shall provide the long-term storage hardware. The Contractor shall be responsible for providing detailed requirements and data storage analysis for the long-term storage solution that satisfies these requirements.

e. All computing resources, application, information management, and information distribution design and configuration are subject to the approval of the Port Authority.
f. All lane equipment hardware performing a like function and of the same part number shall be fully interchangeable without the requirement for physical modifications.

g. The PARCS application software shall remotely monitor all PARCS field equipment. The Port Authority shall monitor the server and network performance and proper operation. The Port Authority shall monitor the server hardware and all network equipment up to the edge devices. The Contractor and other authorized staff shall have access to view all components of the system based on permissions granted by the Port Authority.
h. Each field device shall be assigned a unique identifier within the PARCS that is not shared with any other field device. Should the field device need to be replaced, the replacement field device shall assume the old device's unique identifier. Contractor shall coordinate with the Port Authority to develop the naming convention for the field devices. The Port Authority shall assign all IP addresses.
i. The PARCS configuration shall provide lane autonomy such that no single point of failure of a device shall cause an operational failure of surrounding lane functionality. Equipment at a single lane may fail causing a shutdown of a lane; however, the failure shall not affect other lanes.
j. Contractor shall reuse existing infrastructure where functional and cost efficient, including such items as cashier booths, AVI equipment, etc.
k. Application and Data Servers
    1) All Server hardware components that shall support the PARCS shall be provided by the Port Authority.
    2) The Contractor shall provide detailed hardware requirements that comply with the Technology Standards for the Port Authority (see Attachment K) during the design phase of the project. The Port Authority shall procure, install, and maintain the server hardware.
    3) PARCS Central Servers
        i. The Contractor shall implement a central aggregation software system to aggregate audit, reporting, and business analytics (dashboard) functionality for all four airports. The central aggregation software system shall be the same PARCS interface used for each individual airport, but may have reduced functionality for system administration and management. Operational control of field devices will not be required in these servers. The central aggregation software system shall have all reporting capabilities specified in this document for all four airports.
        ii. The PARCS shall be designed to support stand-alone operations (distributed system with intelligent devices) as well as centralized management of the PARCS for each airport.
        iii. The PARCS Servers shall contain all PARCS database software that is associated with revenue-closeout activity statistics and designated reports.

iv. The application software shall be fully installed and configured on the Servers with all software licenses registered to the Port Authority.

v. The Port Authority shall provide the Contractor with remote access to the PARCS servers and field devices and accompanying PARCS data in accordance with the Technology Standards for the Port Authority attached hereto as Attachment K. The security functions provided by the applications software shall include but not be limited to:

a) Comply with the Technology Standards for the Port Authority (see Attachment K)

b) Comply with NIST, FISMA, and PCI standards for remote access.

c) Where the change and/or update is authorized, the applications software shall log each access to the PARCS system and create an audit trail that includes the following:

- Date/time of change
- Name of User making the change
- Name and IP address of the remote access device making change
- Record of change made
- Record of data modified or changed (prior to change)
- File identities and record count

vi. Contractor shall provide recommended storage capacities required for each component to support the solution.

l. All field equipment and components shall be fully protected from the ambient environment. Operation of the equipment shall not be affected in any way by normal weather conditions experienced at each airport. At a minimum, operation of the equipment shall not be effected in any way by the conditions listed below:

1) Ambient Temperatures: -20ºF to 120ºF (with addition of solar loading)
2) Humidity: 0% to 95% (non-condensing)
3) Rain: Blowing rain with 80 mph gusts
4) Dust: Blowing dust and fine sand

B. Parking Management Control Center

The Contractor shall provide plans for a parking management control center at each airport. The Contractor will review current control centers to determine if they are acceptable for the operation of its proposed system. The control center shall contain workstations and a video wall or equivalent, such that operators

within the Parking Management Control Center can perform the following functions:

I. Review of LPR images
II. Review of exception transactions
III. Provision of customer service via intercom
IV. Exception approvals
V. Review CCTV activities in lane

C. Credit Card Processing Subsystem

I. Approximately 40% of the parking revenue is processed as credit card transactions in the lane or at a POF station. The Contractor's solution shall be certified to process credit card transactions through the Port Authority's current Merchant Banking Services Providers (Bank of America (BAMS) and American Express platform). Should the Merchant Banking Services Provider change, the Contractor shall be required to adjust to accommodate possible changes in the platform utilized.
II. The Contractor shall provide a plan to convert from the existing middleware product from Verifone to another if such is proposed. The Contractor shall provide for Port Authority review the approach and details of the conversion plan, middleware software product and any other third party vendor employed.
III. Credit Card Processing shall follow a Host Capture approach such that when the end of day settlement is performed, only an indication of such, along with balancing of system to settlement house data is required. End of Day settlement shall be based on a virtual end-of-day concept to allow each airport to select the appropriate time to conduct the settlement as fits their business needs.
IV. The PARCS shall accept major credit card types (i.e. credit, debit and prepaid) and the following card brands – American Express, Discover, MasterCard, Visa and Diners Club for payment. For all approved bankcard authorization requests, the PARCS shall provide a credit card transaction receipt if requested by the patron.
V. The PARCS shall provide online real-time authorization for credit card payments made at PARCS point-of-sale devices.
VI. The following types of credit cards/devices shall be accepted at all point of sale devices for parking access and payment at a minimum:
    a. Magnetic-stripe credit cards
    b. EMV Chip credit cards
    c. Contactless Chip credit cards
VII. Contractor shall provide a pay-by-phone application.
VIII. All credit card transactions shall be encrypted from the terminal at point-of-sale and shall remain encrypted for communication to the offsite clearinghouse. The Contractor's credit card interface shall utilize an

approved, commercially available encryption solution, as approved by the Port Authority's Merchant Banking Services Providers and meets PCI standards. All credit card data stored in the database shall adhere to PCI PA DSS standards for encryption.

IX. Contractor-provided aspects of the credit card processing subsystem shall be PCI-compliant, such that no Contractor-provided product or solution shall prevent the Port Authority from achieving total PCI Compliance in its parking operation. The Contractor shall provide a solution that precludes the Port Authority from PCI compliance assessments of the network infrastructure. The PARCS system shall not retain credit card information.

X. Contractor's proposed PARCS shall conform to PCI DSS Version 3.0, or most current version, and the PARCS application shall be PA-DSS certified and PIN Transaction Security (PTS) for PIN transaction devices according to the most recent PCI standards as of the Factory Acceptance Test completion date.

XI. The PARCS solution enables credit card payments to be authorized for the exact amount of parking services being purchased.

XII. Credit card authorizations shall use the Port Authority's existing internet connection and firewall. The Contractor shall submit its network requirements to support concurrent access to the internet to support credit card processing, clearing and settlement through redundant diversely located network communication paths and TEC will design and build the network resources to accommodate. The Contractor shall also submit its requirements to provide a supplemental communications method to ensure that credit card processing, clearing and settlement will proceed without interruption in the event a major network issue prevents such processing through the normal communications path and TEC will design and build the supplemental communications method to accommodate.

XIII. Offline processing of credit card payments is required. Should the fee satisfy a floor limit amount, set by the Authority at each airport, and communications to the authenticator not be operational, the encrypted transaction will be stored for resubmission when connectivity is restored. Communication outages may be of short or long duration. The system must provide a configurable elapsed time parameter to identify when the system considers the communication link is not operational and shift to an offline mode. Transactions stored for future resubmission will reside in an unapproved floor limit queue. Only authorized users with proper security will be allowed to access the queue.

XIV. Where the credit card clearinghouse utilizes multiple IP addresses (or URLs) for clearing redundancy, the credit card terminals shall be configured to send transactions to all of the available IP addresses (URLs) or fully qualified domain names offered by the clearinghouse.

D. Mobile Payment

I. The Contractor shall design the PARCS for patrons to pay with mobile devices. The Contractor shall integrate with multiple modes of payment, including:
   a. Mobile application
   b. Online payments
   c. Pay by phone
      1) Pay by voice
      2) Pay by text

II. The Contractor shall design the mobile payment system to be compatible with multiple payment transaction options, including but not limited to:
   a. Credit card checkout
   b. Reloadable mobile application wallet
   c. PayPal account
   d. Google wallet

III. The Contractor is required to propose advanced system integration that grants patrons access to the parking facility using a mobile device, through technologies such as RFID, QR or barcode scanning.

IV. Mobile payment systems shall be integrated with the PARCS software and perform reconciliation of transactional data in accordance with the Port Authority Audit Checklist.

E. Parking Loyalty Program

I. The Contractor shall provide a Loyalty Program application for its customer loyalty programs including; frequent parking patrons, *E-ZPass® Plus™* AVI users, reserved parking patrons and users of the prebooking/prepayment module, among others.

II. The application shall be a web-enabled program.

III. The application shall provide login to users external to the Port Authority's website.

IV. The application shall establish a secured parking account set up on a third party hosted application.

V. The parking account information shall be hosted off-site by a third party. The account information shall include as a minimum, the patron's name, address, contact phone numbers, vehicle make, model, license plate number, account type (frequent parker, *E-ZPass® Plus™* AVI, reserved parker, etc.,), email account and credit card number and expiration date.

VI. If the account type is a frequent parker, the parking patrons shall receive a number of free parking days based upon "points" accumulated for the number of days parked. The Port Authority patron shall decide when to use the frequent parker points. If the account type is an *E-ZPass® Plus™* AVI user or a reserved parker, each parking stay at the Port Authority, for each exit event, a credit card on file shall be charged for the parking stay. The credit card holder shall receive an alert one (1) month before the credit expiry date

and shall be automatically blocked if a replacement card is not entered into the cardholders account.

VII. While a third party shall host the accounts, all parking charges shall also be posted within the Port Authority PARCS. All parking revenues shall be posted as gross. The third party fee for each parking charge shall be posted within the PARCS as a credit (deducted from) to the parking revenue posted for each transaction.

VIII. All parking transactions shall be recorded within each patron's account(s) and monitored by the system.

IX. Any parking transaction shall automatically trigger an email to the patron thanking him/her for the business. The email shall be a template defined by the Port Authority.

X. The application shall provide for up to 999 different templates to be defined by the Port Authority.

XI. The Port Authority shall use the database for marketing purposes, to initiate emails and/or letters encouraging patrons to use a coupon or marketing initiative based upon any marketing program defined by the Port Authority.

F. PARCS Workstations

I. Contractor shall provide minimum recommended requirements of workstations where they differ from the Port Authority standards.

II. Any workstation shall access any module of the PARCS based on access rights of the user including PARCS, PSCS, LPR, Employee, AVI or Proximity Access System, reporting, etc.

III. Granularity of these permissions shall also include separate read only, read/write privileges.

G. Entry Stations

I. Currently Attachment I lists locations and counts for each airport. This may change slightly when the Contractor begins installation due to ongoing construction at the airports.

II. Each Entry Station shall consist of the following components and capabilities:
   a. Meets ADA requirements and standards
   b. The equipment will be protected with appropriate tamper-resistant locking system (all entry stations keyed alike, and unique to this facility)
   c. Functionality required is as follows:
      1) Provide RFID capability in selected locations for Bus and Employee access via HID tags.
      2) Provide AVI for *E-ZPass® Plus™* functionality on entry.
      3) Accept magnetically encoded credit cards.
   d. When applicable, issues one credit card-sized, barcoded parking ticket for each entry transaction.

e. Entry Station ticket slot or EMV reader shall be able to read an ISO standard side-stripe magnetically encoded card such as a credit card
f. Pinhole camera to activate upon activation of intercom or at the start of each entry traversal, regardless of the type of credential presented.
g. Inserted credit cards shall be read in a minimum of two (2) directions
h. Provide an active color matrix message screen that is easily readable in all ambient lighting conditions. Sample of this screen shall be provided with the Contractor's Proposal Response
i. Utilize visual instructions for patrons to understand the sequence of events to complete a transaction without the need to read English
j. Issues configurable audio voice instructions to compliment the visual instructions, if activated
k. Push-button or touch screen ticket issue with configurable setting to automatically issue a ticket based on loop detection
l. Illuminated ticket slot
m. Push-button intercom integrated into the face of the Entry Station (propose VoIP intercom solution)
n. Retractable ticket mechanism which enables tickets to fall into a container marked as retracted if not pulled within a configurable time frame (default is fifteen (15) seconds)
o. Uniquely encoded parking tickets printed for each specific parking area with specific information printed: Ticket number; Date/time of entry; lane number; traversal number.
p. Computerized Lane Control and Interface Processor (LCIP) to control equipment component communications within the lane and to the Servers utilizing appropriate communications
q. Stand-alone capabilities for each Entry Station in the event that network communication to the host is lost, and regardless of where on the network the communication interruption occurs. Specifically, each Entry Station shall provide offline transaction storage capacity for all transactional information for a minimum of seven (7) consecutive days. Credit Card In functionality shall be disabled while in an off-line mode. The lane shall automatically close in the event that the maximum transaction threshold is reached and shall remain closed until reestablishment of communications. Entry Station shall automatically upload all transaction information to the Servers once communications is restored. Entry ticket information shall also be sent to all exit stations in the lot if communications to them is available.
r. Bar code/QR code reader to read either paper or electronic (smartphone) bar code and QR code.
s. Ticket Stock Low alarm generated in PARCS central software
t. Ticket Stock Out alarm generated in PARCS central software
u. Ticket Issuing Machine Open alarm generated in PARCS central software

III. As part of its Proposal, the Contractor shall submit product data of proposed Entry Stations.
IV. The Contractor shall propose an optional entry station that allows processing for vehicles traveling between parking facilities or to nested areas within parking facilities.
V. Entry lanes shall utilize existing infrastructure where available.
VI. Provide automated and manual controls for the Red/Green lights.

H. Cashier Stations

I. All cashiered lanes shall be dual-use such that they operate in a cashiered mode through the cashier station when a cashier is present or in an un-manned mode through the Express Exit station or transaction panel when a cashier is not present. The cashier station operating in un-manned mode shall operate in the same manner as an Express Exit lane.
II. Each cashier station shall be equipped with the following components:
   a. Meets ADA requirements and standards
   b. Cashier terminal (computerized device that shall operate the exit cashiering functions) with integrated credit card functionality. Cashier stations shall have a configurable screen timeout setting.
   c. Ticket reader/validator that accepts ISO standard readable cards, magnetic stripe or barcode parking tickets, validations, and credit cards through the same single slot. Note: EMV credit card reader may be a different device.
   d. Cashier terminal shall read bar codes and QR codes from a cell phone or from hard copy.
   e. Ten key pad for entry of PIN
   f. Duress alarm – this alarm may be provided as a separate, standalone device
   g. Touch screen cashier monitor supplemented with standard QWERTY keyboard and mouse
   h. In booth ticket and credit card readers to supplement the external readers shall be provided for use by cashiers.
   i. An in booth printer to be used for receipts when requested by the cashier and for shift close or suspend summary data.
   j. PARCS shall process all acceptable payment methods: (Cash, CC, Mobile device (cell phone), *E-ZPass® Plus™*
   k. PARCS shall have the ability to cancel a credit card or cash and credit card transaction only before the credit card is ingested into the ticket transport mechanism
   l. Inside booth for cashier and external for patron Intercoms using VoIP
   m. Receipt printers (one patron facing and one in cashier booth) to produce receipts for a transaction. Duplicate receipt function shall be a user selectable feature that can be disabled. Receipt printer inside cashier

booth shall automatically be disabled in unmanned mode. Customers shall be given the option for a receipt for all transactions (no auto-issued receipts

1) Upon successful payment and if customer has requested, print a receipt that includes:
   i. Port Authority brand-logo and address
   ii. Receipt #/Transaction #
   iii. Time, date and lane in/out
   iv. Length of stay
   v. Parking fee
   vi. Total amount
   vii. Method of payment
   viii. Amount paid
   ix. Change Due
   x. Breakdown of charges by time and rate
   xi. Cashier ID#
   xii. License plate number
2) The receipt shall be configurable and include multiple lines of up to 160 characters of custom language at the bottom provided by Port Authority designated personnel.
3) The Port Authority shall have the option to change receipts for all (cash/credit card) transactions to be auto issue or by request. This function shall be a parameter driven changeable by Port Authority staff with appropriate privileges.

n. The PARCS shall implement cashier booth patron fee displays that are easy to read in all ambient light conditions, LED – type mounted on the exterior of the cashier booths.
o. Dual cash drawer operation (relief cashier shall operate out of a separate cash drawer) with removable, lockable inserts. All cash drawers to be keyed.
p. Upon cashier log out, the lane shall be able to switch to Express Lane exiting through the use of the Transaction Panel.
q. Stand-alone capabilities for each Cashier Station in the event that network communication is lost, and regardless of where on the network the communication interruption occurs is required. Specifically, each Cashier Station shall provide offline transaction storage capacity for all transactional information, including storing encrypted credit card data, for a minimum of twenty-eight (28) consecutive days. The lane shall automatically close in the event that the maximum transaction threshold is reached and shall remain closed until reestablishment of communications. In the event the network outage occurs frome the server to the authenticator, the transactional encrypted data shall also be stored in the server. The Cashier Station shall automatically upload all

transaction information to the Servers once communications is restored if not already done so.

1) In the event that the device's offline storage capacity is filled, and the device needs to shut down, all stored data shall be permanently stored and accessible once the device is powered on.
2) In the event that a device is operating in off-line mode and on UPS power, the device shall permanently store all information prior to shutting down in the event that the UPS battery power is depleted.

r. The Cashier Station shall alert cashier when the transaction threshold is nearing allowing the cashier to prepare the lane for closure.
s. The Swipe Credit Card reader shall be integrated into the transaction panel

III. In the event of an emergency, the cashier shall be able to open the drawer and open gate without requesting for a supervisor (police or other)

IV. As part of its Proposal, the Contractor shall submit product data of proposed Cashier Station CCTV and Audio/Visual Functionality. If possible, the Contractor shall reuse the existing CCTV in-booth cameras at both JFK and LGA.

CCTV cameras and microphones shall be installed within each cashier booth to capture interaction between the cashier and the patron or to capture the interaction of the patron to the lane equipment when the lane is operating in an unmanned mode. The image and audio shall be tied to each transaction. All cameras and audio shall be synchronized with the traversal, and be associated with the transaction. The PARCS application software shall store CCTV data based on the limitations of the server hardware provided by the Port Authority. If possible, the existing CCTV cameras in LGA and JFK booths shall be reused; currently installed are Nextiva Dome Cameras and Verint servers.

I. Transaction Panel

The Transaction panel contains the hardware facing the patron on exiting the lot. All exit lanes with a booth shall be equipped with a Transaction Panel.

Installed in the Transaction panel shall be the following:

I. A ticket reader/validator shall be installed in the sidewall of the booth in a location where the patron can interact with a cashier if necessary.
II. Shall have a receipt printer with large control button for patron to request a receipt.
III. Shall meet all ADA requirements and standards
IV. Shall have a Cancel button that allows a patron to cancel a transaction once a parking ticket has been inserted but before any payment has been made.

Upon activation of the cancel button, the parking ticket shall be returned to the patron.

V. Shall contain a Pinhole camera to activate upon activation of intercom or at the start of each Traversal, regardless of the type of credential presented. The system shall have some form of facial recognition capability such that it knows which picture taken shows a face and should be kept.

VI. Shall provide a Push-button intercom, integrated with the camera and installed in the face of the Transaction Panel (reuse existing audio cabling and intercom head end equipment or propose new VoIP intercom solution).

VII. Shall Provide a Contactless Credit Card reader integrated into the face of the Transaction Panel.

VIII. Shall Provide Barcode and QR code reader(s) for reading coupons, tickets, and electronic visual display integrated into the face of the Transaction Panel.

IX. The Transaction panel shall fit in existing booth with minimal modifications to booth.

X. Shall have a Patron Fee Display.

XI. The Transaction Panel shall have the following functionalities:

a. Shall accept ISO standard readable cards, barcode parking tickets, validations, and credit cards.
b. Inserted credit cards shall be read in all four (4) directions.
c. Shall have an Illuminated ticket slot and ticket reader.
d. The Transaction panel printer can be used to print a patron receipt that requires no signature on request of the patron and/or a credit card voucher. The inside booth printer can be used by the cashier to print the same information should the outside printer be inoperable. All customer receipts shall be issued through the transaction panel, in unmanned mode.
e. Upon successful payment and upon patron request via a large, highly visible push button, print a receipt that includes the information identified in 1.05 H.M above. The receipt shall be configurable by Port Authority designated personnel and include multiple lines of up to 160 characters of custom language at the bottom.
f. The Port Authority shall have the option to change receipts for credit card transactions to be auto issue or by request. The configurable timeout function for receipt request shall be initially set for twenty (20) seconds or until the gate closes.
g. A Receipt Stock Low alarm shall be generated on FMS while in unmanned mode
h. A Receipt Stock Out alarm shall be generated on FMS while in unmanned mode
i. The Patron fee display must be easily read in direct sunlight and at night with ambient lighting. The color matrix display shall have a minimum size of six (6) inches measured diagonally. Display shall have brightness and

contrast controls to allow a patron easy viewing and recognition of information under all lighting conditions.

j. Utilize visual instructions for patrons to understand the sequence of events to complete a transaction.

k. Issues audio voice instructions on to compliment the visual instructions. Audio voice instructions shall be configurable for being turned on or off.

J. Express Exit Stations

The Contractor shall provide the ability for any exit lane to be a manned lane accepting all forms of payment, or an Express Exit lane. This would include ensuring that necessary lane signage is changed appropriately. Additionally, the Authority shall at times dedicate an exit lane in a lot to a specific client. The lane signage shall be able to so identify such a lane. An Express exit station shall contain the same hardware installed as a manned Cashier Station with the following functional differences:

I. Each Express Exit Station (unmanned lane) shall be equipped with the following capabilities above those of manned cashier stations:

II. Express Exit lanes will not accept cash, paper vouchers or paper discount coupons.

III. LPR confidence level must be above 80% (n-3). If not a supervisor either remotely or in the plaza must correct the LPR.

IV. If a valid *E-ZPass® Plus™* Tag is read the system will identify the class of the vehicle based on the LPR and tag and apply the appropriate rate table. *E-ZPass® Plus™* will be used first to satisfy the payment unless there is an issue with LPR, tag number or ticket which would require supervisor intervention. The patron will be allowed to present another form of payment such as credit card or mobile payment in this situation using one of the acceptable devices in the Transaction Panel within 20 seconds. This length of time will be modifiable by designated personnel.

V. POF payments will be automatically applied.

VI. Paper vouchers, discounts, etc. will not be accepted.

VII. As part of its Proposal, the Contractor shall submit product data of proposed Express Exit Stations.

K. Entry and Exit Lane Vehicle Detection Devices and Barrier Gates

I. Saw cut or embedded loops are currently used for entry and exit lane vehicle detection. The Contractor may suggest alternate means of vehicle detection for consideration.

II. The Contractor shall provide a listing of all existing loops and loop detectors, which need replacement with comparable sensor technology. The Contractor may propose a complete replacement with explanation for review and approval.

III. Entry Lane Vehicle Detection: Entry lane vehicle detectors shall detect vehicular presence, legal entry, illegal exit, stolen tickets and back-outs.
IV. Exit Lane Vehicle Detection: Exit lane vehicle detectors shall detect vehicular presence, legal exit, illegal exit, reverse traversal and back-out.
V. The loop detector shall contain two fully separate, self-tuning, vehicle loop detectors and directional logic circuitry.
VI. The loop detectors shall each incorporate a sensitive Tailgate Recognition System shall resolve two (2) automobiles within six (6) inches of each other on a standard 2.5 ft. W x 6 ft. loop.
VII. The loop detectors shall each operate in multiple separate sensitivity modes.
VIII. Different sensitivity settings shall allow vehicles of varying height and size to be properly detected.
IX. The loop detector shall be fully microprocessor-based.
X. Each detector shall continuously retune itself to its loop frequency during non-detect periods to prevent the detector from generating a false detect output due to frequency variances caused by environmental effects or other factors. Analog type detectors requiring periodic manual tuning or any type of detectors that do not retune unless a manual function is performed shall be unacceptable.
XI. The loop detector shall generate two (2) loop frequencies. No two (2) frequencies shall be the same. This shall minimize the possibility of detector crosstalk or interference between two (2) detector loops mounted within close proximity. Detectors generating an identical frequency shall be unacceptable.
XII. All barrier gates referenced in these Functional Specifications shall contain the following:
    a. Direct drive mechanism
    b. Aluminum gate with padded arm (articulating gate arm as appropriate)
    c. Electronically controlled rebound feature. Gates will not hit people or vehicles in their descent. The method(s) to be used must be provided in the response to the RFP.
    d. Non-resettable, mechanical gate action counter mounted in the barrier gate housing
    e. Gate arm lengths to meet the needs of the specific exit lane such as car or bus lanes.
    f. Single piece gate arm where possible
    g. Break away gate bolts
XIII. Barrier gates shall have sufficient power/resistance to ensure they cannot manually be forced open except when there is no power to the gate.
XIV. Barrier gates shall have a local open and close button mechanism to allow manual open/close of the gates.
XV. Barrier gates installed at the entry lanes shall remain in the closed position in an event there is a power failure and the UPS is no longer able to provide sufficient power to operate the lane.

XVI. Barrier gates installed at the exit lanes shall fail to the closed position in an event there is a power failure and the UPS is no longer able to provide sufficient power to operate the lane.

XVII. As part of its Proposal, the Contractor shall submit product data of all proposed barrier gates.

XVIII. Barrier gates shall be installed utilizing existing infrastructure where possible.

L. Lane Open/Closed Signs (Lane Status Lights)

I. The Contractor shall provide Lane Open/Closed Signs.

II. Lane Open/Closed Signs shall be LED type with the word “OPEN” in green letters and the word “CLOSED” in red letters. Details for additional text or graphics shall be discussed with and approved by the Port Authority. Lane Open/Closed Sign shall be easily readable in all ambient lighting conditions from a distance of 200 feet and a minimum viewing angle of 120 degrees.

III. The message displayed by the Lane Open/Closed Sign shall be controlled automatically by the entry/express exit station. When the entry station is in operation, the Lane Open/Closed Sign shall automatically be set to “OPEN”. When the entry/express exit station is out of operation the Lane Open/Closed Sign shall be automatically set to “CLOSED”. When the entry/express exit station is set into a maintenance mode, the Lane Open/Closed Sign shall automatically be set to “CLOSED”.

IV. For the public entry lanes, the sign matrix size shall be proposed by the Contractor to fit within the geometric circumstances of each location. Minimum character height shall be 5”.

V. As part of its Proposal, the Contractor shall submit product data of the proposed Lane Open/Closed Signs.

M. Uninterruptible Power Supplies

I. Conditioned/emergency power through the TCP/IP-enabled UPS units shall be provided for the following components and facilities to protect components from loss of power, power spikes, and power sags:
   a. Public entry lanes
   b. Public cashiered exit lanes
   c. Public Express Exit lanes
   d. POFs
   e. FOICs (Fiber Optic Interface Cabinets)

II. UPS battery back-up for all lanes shall be sized to last sixty (60) minutes before starting a shut down procedure.

III. An on-line, solid state UPS shall provide both backup power and transient surge protection as defined as necessary by the CBEMA. The Contractor shall be alerted to the fact that there are a number of power distribution panels providing electrical service Port Authority wide. The Contractor shall be

responsible for providing the UPS backup requirements for each of the locations where UPS backup is required, based upon the equipment that is actually being supplied by the Contractor. The Port Authority shall review and approve the UPS units to be provided by the Contractor. The Contractor shall test all UPS system components during the LATs and Site Acceptance Tests for each parking lane/facility. The UPS shall be sized with 50% spare capacity. This shall facilitate 30% expanded load with an 80% continuous load factor.

IV. A single UPS unit, appropriately sized, shall support all devices at an individual entry lane or exit lane with the exception of cashier booth HVAC units.

V. All UPS units shall be SNMP compatible to allow automated notification when battery power is activated or the battery levels become critically low. On-line communication using an appropriate UPS monitoring software application shall be provided on one or more workstations with user selectable options to view the status of each individual installed UPS unit. At a minimum, the monitoring software shall display the operational status of each UPS unit (line/battery, online/offline) and generate alarms in the event the UPS unit's battery power is activated, becomes low or is completely exhausted.

VI. As part of its Proposal, the Contractor shall submit specification sheets of all proposed UPS devices and UPS monitoring software. Included in the UPS product data shall be the manufacturer's recommended battery refresh cycle.

VII. The Contractor shall provide UPS devices

N. Dynamic Signs

I. All dynamic signs shall be LED type. The sign types include:
   a. PSCS Dynamic Signs (Monument) – dynamic signs at entry plazas or level changes that depict the status for each facility or level by displaying "OPEN" in green or "FULL" in red, or providing parking space availability numbers.
   b. PSCS Dynamic Signs (Ceiling-Mounted Directional) – dynamic signs within parking facilities that depict the status for each level or zone.
   c. Exit Lane Dynamic Displays – dynamic signs at exit plazas that depict the status of the exit lane.

II. The Contractor shall be responsible for any and all mounting bracket analysis, design, fabrication and installation required to install the signs. Location of post-tensioning cables, pre-stressing cables and reinforcing steel shall be performed to ensure these structural elements are not affected or damaged.

III. The Contractor shall provide the appropriate controller and software for the each Display such that the message being displayed can be remotely controlled via any workstation with access to the PSCS.

IV. As part of its Proposal, the Contractor shall submit product data and photographs of all proposed PSCS Dynamic Signage.

V. PSCS Dynamic Sign (Monument)
   a. The Contractor shall provide nine (9) Monument Dynamic Signs to communicate pertinent facility information.
   b. Each monument sign shall display space availability for each level of the parking facility.
   c. Proper sign matrix size shall be proposed by the Contractor to fit within the geometric circumstances of each installation location. Minimum character height shall be 5” and shall display either, “OPEN”, “FULL”, or the number of available spaces.
   d. The Contractor shall be responsible for the design and coordination of manufacturing of all Monument Dynamic Signs. The Contractor shall submit the Monument Dynamic Sign design and specifications to the Port Authority for approval prior to manufacturing. Each location shall be submitted separately as the number of necessary dynamic panels shall vary from location to location.

VI. PSCS Dynamic Sign (Ceiling-Mounted Directional)
   a. The Contractor shall provide one hundred forty-eight (148) Ceiling-Mounted Directional Dynamic Signs to communicate pertinent facility level and zone information.
   b. Proper sign matrix size shall be proposed by the Contractor to fit within the geometric circumstances of each installation location. Minimum character height shall be 5” and shall display either, “OPEN”, “FULL”, or the number of available spaces.
   c. The Contractor shall be responsible for the design and placement of each Ceiling Mounted Directional Dynamic Sign. The Contractor shall seek and receive written approval for sign design, specifications, and approval prior to manufacturing.

VII. Exit Lane Dynamic Displays
   a. The Contractor shall provide Exit Lane Dynamic Displays to show the status of the exit lane.
   b. The Contractor shall replace the existing Exit Lane Dynamic Displays. Proper sign matrix size shall be proposed by the Contractor to fit within the geometric circumstances of each installation location. The Contractor shall be responsible for any and all mounting bracket analysis, design, fabrication and installation required to mount the signs to the existing canopy structure.
   c. The Contractor shall provide the appropriate controller and software for the Exit Lane Dynamic Display such that the message being displayed can be remotely controlled via any workstation with access to the PARCS.

O. LPR System

I. A LPR system shall be installed at the Port Authority as part of the PARCS replacement project in all public entry and exit lanes.
II. The LPR system shall not place an undue burden on communications performance. As such, each lane shall use a camera with built in controller logic to select the best pictures (Infrared and CCTV) for transmission to the airport PARCS server.
III. The Contractor shall propose an LPR solution, which indicates whether to locate LPR controllers servers centrally or at the lanes.
    a. If the proposed LPR solution utilizes virtual machines centrally-located in the Authority's data centers or airports, the Authority shall provide those virtual machines and, at the time of Proposal, the Contractor shall submit the detailed virtual machine requirements and required network bandwidth between each entry and exit plaza and the Port Authority data centers.
    b. If the LPR servers are located at the lanes, the Contractor shall furnish, install and maintain all LPR system server hardware at the time of System installation.
IV. The system shall be able to retrieve entry information at an exit lane and/or POF during loss of communications to the servers. The Contractor will propose the methodology to be used to accomplish this.
V. Throughout this Section, the term "LPR database" shall refer to a generic database(s) that may be housed entirely or in part on the PARCS central databases and/or on the LPR Subsystem hardware or other devices as specified by the Contractor.
VI. The LPR Subsystem shall consist of all hardware and software necessary to provide a complete and functional LPR subsystem that achieves the Port Authority's required functionality and accuracy percentages, and that does not adversely affect any function of the PARCS.
VII. The Contractor shall be responsible for providing a LPR subsystem that is fully interfaced and integrated into the PARCS. This integration shall include linking the LPN captured at entry to the unique ticket identification (or other entry credential information) for every transaction. Should the entry information need to be obtained at an exit station to process the transaction (i.e. lost ticket, unreadable, etc.), both the LPN and ticket shall be removed from their respective active (open transaction) inventories once the vehicle has exited.
VIII. The LPR database shall be used to conduct automated searches and queries for special circumstances, such as outstanding balances, unresolved incidences, and prior entries with no exits, Gray List, and police requests.
IX. LPR images and CCTV camera images shall be maintained in the active database for the same duration as all other transactional information.
X. The LPR system shall keep a "Gray List" of exception transactions based upon vehicle LPN information. Exception transactions shall include insufficient fund transactions, lost ticket transactions, swapped media transactions and

passback violation transactions. The list of exception transactions shall be updatable by authorized personnel. This Gray List shall reside on the PARCS server system's database. As an exception transaction is processed, the LPN and corresponding transaction information shall be recorded as part of the Gray List record. Entries in the Gray List may be used to deny entry or exit based on the entire list or specific entries in the list.

XI. LPR shall acquire an image of a vehicle's entire license plate at a ninety-five percent (95%) rate for all non-exception vehicles as defined within this section.

XII. The LPR system shall achieve an N Factor rating of ninety (90%) meaning specifically that the system shall read all license plate characters, exclusive of stacked characters, correctly ninety percent (90%) of the time for all non-exception vehicles as defined within this section. Missing, misread, or additional characters as determined by the LPR Subsystem shall be counted against the read accuracy. (i.e. if a license plate contains six standard characters "ABC123", then N=6. Therefore, in order for the system to achieve an N read, the system shall return the LPN "ABC123" exactly). Additional characters added before or after the license plate characters shall count against the read rate. (i.e., "1ABC123" would not constitute an N read.) The N factor shall be configurable by airport or by lot.

XIII. Exception vehicles shall not count against the accuracy of the LPR system. For the purposes of the LPR performance requirements, an exception vehicle is defined as:

a. Any vehicle whose license plate is obstructed, obscured, or encroached upon by a foreign object (having a foreign object within .375 inches (⅜") of any LPN character).
b. Vehicles with no license plate
c. Vehicles with temporary cardboard (non-reflective) "Dealer Plates."
d. Motorcycles

XIV. The LPR system shall check the license plates of vehicles entering the facility and compare those plates against the hot-lists downloaded from the various Law Enforcement systems. When a match is found, the LPR system shall issue an alert to Authority-designated agents, based on the hot-list where the match was made, the details of which will be finalized as part of the Technology discussions during the design phase of the project.

XV. LPR Cameras

a. The Contractor shall provide LPR cameras for all entry and exit lanes:
b. The Contractor shall furnish and install image capture cameras including any sensor-activated lights or shade canopies necessary at all public entry and exit lanes to provide system functionality. Technology exists to have the image and LPR cameras merged into a single camera. The Contractor may propose this as part of their solution.
c. Devices shall be placed in theft deterrent and vandal resistant housings that meet applicable code requirements for outdoor equipment.

d. The Contractor shall determine the exact location of each device and utilize existing infrastructure.
e. All entry images shall be post-capture, meaning that the cameras are placed in such a position that a vehicle's LPN is photographed after the entry credential issuance to the patron or accepted by the system.
f. All exit images shall be pre-capture, meaning that the cameras are placed such that a vehicle's LPN is photographed before the patron presents their parking credential at the exit.
g. The preferred method of illumination for license plate capture is infrared light.
h. As part of its Proposal, the Contractor shall submit product data of the proposed LPR cameras.

XVI. The LPR subsystem shall read all plates, reflective and non-reflective, from the at least the following states:
a. New York
b. New Jersey
c. Pennsylvania
d. Connecticut
e. Massachusetts
f. Maryland
g. Virginia
h. Florida

XVII. LPR Image Review Workstations (IRWs)
a. Access to the LPR system shall be via a web browser on IRW hardware that shall be provided by the Port Authority, and installed at each airport Parking Management Office and/or Command Center. The PARCS shall include a web-based IRW component to enable an operator to review images for manual read and data correction into the LPR database. The PARCS shall support up to 75 concurrent IRW operators (subject to available hardware provided by the Port Authority) at each airport. The LPR number read and the image shall also be displayed on the IRW screen for correction.
b. When any LPR exception occurs, it shall be displayed as a high priority alarm on all logged-in system workstations at the same time. Once an LPR exception is resolved from any workstation, the alarm shall instantly be removed from all system workstations. This function shall be configurable so that the alerts can be modified for specific users or user level.
c. Exceptions would occur if there is no LPR read or the LPN read falls below a confidence level settable by authorized personnel. The default confidence level shall be proposed by the vendor, at the time of proposal, and approved by the Authority. For all exceptions, the system shall present the image of the vehicle along with the LPN for review.
d. Exit traversals in un-manned and express lanes shall be shown in a separate list from all other LPR exceptions and given higher priority than

all other traversals for review and correction. The LPR number read and the image shall also be displayed on the cashier terminal screen for correction. Note that for reporting the confidence level reported by the system shall be used and not the corrected number.

e. On exit the LPN, still image of vehicle, entry identifier (i.e. ticket number), date/time of entry, entry lane shall be presented shown on the cashier terminal based on the entry LPN in the database. Once the identifier (ticket) is read the system shall display similar entry information based on that identifier.
f. Entry lane LPR reads shall be reviewed and corrected after the fact; that is after the vehicle has entered the parking facility. As many patrons shall leave the facility within one hour these need to be reviewed and corrected in a timely fashion. Entry traversal LPR images up for review shall be placed into a single queue and be dispatched to the LPR Review Workstations that are active. Exit review shall be given priority over entry reviews. All LPR corrections shall be logged by user, time and date.
g. License plate images that fail to match the numbers that are captured at entry shall be alarmed into an IRW for correction
h. Authorized users shall use the IRW to enable remote processing of exception transactions (e.g. Lost Ticket, Mutilated, Unreadable, etc.) at all Cashier Stations and Express Exit Stations. The authorized user, who shall be identified by the Authority, shall use the LPR data sent from the lane to the IRW to verify entry information and transmit the entry information to the exit station for automated calculation of the appropriate parking fee. Remote exception processing shall cause the Cashier Station or Express Exit Station to generate and swallow an exception ticket for audit purposes.

P. Parking Space Count System (PSCS) (optional)

The Authority shall decide whether it wishes to install PSCS in its garages at a later time. The Contractor shall provide pricing in its proposal for PSCS in each garage. Should the Port Authority decide to install the PSCS, it shall be done at the prices set forth by the Contractor in the Pricing Sheets, accepted by the Port Authority. See Attachments C1 and C2 for proposal pricing information.

I. The Contractor shall provide a PSCS system along with required infrastructure.
II. The PSCS shall be integrated into the PARCS such that the available parking spaces within a garage or lot by the PARCS are maintained in real time.
III. The Contractor shall price in its proposal cost estimates for the Authority the following types of PSCS:
    a. Space by Space – All available spaces in the facility are monitored and reported on.

b. Row by Row – The number of spaces reported on in a row is determined by the number of entries and exits in a row.
c. Level counting – The number of spaces in a level is reported on and determined by the net of entries and exits to a level.

IV. The PSCS shall ensure that the count of vehicles into and out of the parking facility matches the total of all occupied spaces reported by the PSCS

V. For Space by Space and Row by Row approaches, the system shall be able to differentiate spaces as normal, reserved, charging station and handicapped. Should additional categories be introduced the system must be able to differentiate and report on them as well.

VI. Garages with space-by-space detection shall include dynamic signs at the ends of aisles to provide parking availability information to patrons on main drive aisles. The Contractor will propose quantity and location of space availability information for the patrons via signs or other means. The quantities of space availability signs in this specification are an estimate only and shall be used for comparison of cost values among vendors.

VII. Garages with space-by-space detection shall display red/green lights over every space to indicate space availability. The configuration of lights and detectors shall be proposed by the Contractor. The Contractor shall provide a different location for roof top signs.

VIII. Garages with space-by-space detection shall provide a means to identify a specific vehicle to assist patrons with lost vehicles.

IX. The system shall be able to communicate capacity for a garage level and at a lot level as required with Port Authority and approved public web sites.

X. The PSCS shall provide the following:
a. automatic and manual control of the status of the space count signage
b. automatic update of the number of parking spaces available on dynamic signs every ten seconds; frequency of update up to 30 second intervals shall be configurable by the Port Authority
c. maximum and minimum counts for each parking facility
d. hourly flow rates through entries and exits
e. receipt of input signals from the entry and exit lanes for valid entries and exits
f. control of the Dynamic Signage that supports the PSCS
g. Contractor shall design, furnish and install any additional infrastructure that the PSCS requires and
h. Communication to the Port Authority's website to upload parking availability in configurable time increments, including real time, for public viewing as well as a Contractor provided Mobile application. Port Authority shall provide Contractor the required file format for providing this information.

XI. The PSCS shall be fully automated with no Port Authority intervention required under normal operating circumstances. While in operation, there

shall be allowances for manual adjustments and override of the PSCS via the workstations, including but not limited to:

a. establishing the initial number of parking spaces within each parking facility
b. setting parking space variance values
c. manual control of all parking space count dynamic signs
d. adjustment of the number of spaces available within each parking facility, and
e. reconciliation after a survey or inventory by authorized user.

XII. Workstation Functions

a. All data required to monitor, and adjust the PSCS shall be available on system workstations. The PSCS workstation functionality shall be made available on all PARCS workstations for authorized personnel to access. The screen formats shall be designed for the Port Authority's parking configurations (layout). It is desired that all screen formats for the PSCS purposes shall reflect the physical layout of the Port Authority's parking facilities for ease of associating the displayed data with physical conditions. The Contractor shall submit proposed screen layouts for the PSCS for approval thirty (30) calendar days prior to system implementation. Any change in the configuration screen formats shall be subject the submittal approval process.
b. Workstation application shall include the following:
    1) Web-based GUI, no workstation-specific software installation required.
    2) GUI, real-time graphical displays of the parking surface lots with both the number of available parking spaces and spaces occupied (immediate user identification of count status). Red = Full; Yellow = Approaching capacity; and Green = Spaces Available;
    3) Alarms shall be configurable by Port Authority staff with appropriate rights and privileges.
    4) Alarms to notify when a facility, level or row is "FULL" or nearing full;
    5) Alarms of component failures;
    6) Operating status of all dynamic signage, including message currently being displayed;
    7) Display of summary statistics of parking space availability by specified date/time period.
    8) Integrated with the PARCS software for availability and turnover reporting as well as dynamic pricing.
c. The Port Authority shall determine the maximum number of vehicles that a parking facility shall accommodate. The Port Authority shall be able to adjust the configurations (spaces, rows), numbers of handicapped, reserved, charging stations and total parking spaces for each parking level and parking facility as a whole.

d. An inventory of a surface lot shall provide an exact count of the vehicles in surface lot. Provisions shall be included to manually adjust count information into the PSCS. Information from a mobile LPI system which shall provide a space by space count with LPN shall be uploadable to the PSCS. The spaces and row configurations between the two systems need to be reconcilable.

XIII. PSCS Capacity Requirements

The PSCS shall be designed to accommodate all parking spaces within all surface lots and garages that are part of this project regardless of how those spaces are assigned. The system shall have sufficient capacity to control all detectors, status signs and other devices for all parking facilities. The system shall incorporate capacity for space control and detection for expansion of the number of parking spaces and ingress/egress points.

XIV. Operational Procedures

a. "Vehicle Count" shall be the number of vehicles located in a parking facility. "Spaces Available" is defined as the unoccupied general use spaces in any given facility resulting from the number of vehicle counts affecting the space availability and shall be able to differentiate between general categories of spaces.
b. For each parking facility, the system shall receive input from the PARCS at each entry lane and at each slip lane between parking lots if installed. As a vehicle enters or exits a parking facility, a valid event shall cause a signal to be dispatched to the PSCS software. The PSCS shall record the event and adjust the number of available parking spaces accordingly

XV. Parking Space Count System Hardware

a. All PSCS dynamic signs shall be LED type. The sign types include: Facility Open/Full Sign/Count Sign – dynamic that depict the status for each facility by displaying "OPEN" in green, "FULL" in red, "CLOSED" in red, or the number of available spaces in green. Abbreviations proposed due to space limitations shall be reviewed and approved by designated Authority personnel.
b. Proper sign matrix size shall be proposed by the Contractor to fit within the geometric circumstances of each installation. Minimum character height shall be as follows:
    1) Facility Summary Level Status Sign – 5"
    2) Individual Level Status Signs – 5"
c. The PSCS software shall control the message that is displayed on all signs.
d. The PSCS shall allow the Port Authority to override the status displayed and to change the predetermined occupancy number that triggers a change from one sign display to another displayed status.
e. As part of its Proposal, the Contractor shall submit product data and photographs of all proposed PSCS Dynamic Signage.

XVI. PSCS Vehicle Detection Subsystem

a. The Vehicle Detection Subsystem shall utilize vehicle detectors and data controller to support the PSCS required functionalities.
b. Vehicle detectors quantities and locations shall be proposed by the Contractor. Vehicle detectors shall be installed by the Contractor.
c. Vehicle detectors shall be located such that vehicular movements relative to entering and exiting a parking facility and traversing levels and rows are detected as required above.
d. Each vehicle detector shall provide 99% accurate detection for vehicle counts.
e. The vehicle count inputs shall be transmitted to the Servers that shall process the data on a real-time basis. The count signal shall be received within one second from the event. Counts shall be manually adjustable from a user workstation.
f. The following functional requirements of the PSCS shall be provided using vehicle count data:
    1) automatic and manual control of the status of the space count signage,
    2) automatic update of the number of parking spaces available on dynamic signs every ten seconds; frequency of update up to 30 second intervals shall be configurable by the Airport,
    3) historical maximum and minimum counts for each parking facility,
    4) hourly flow rates through entries and exits, and
    5) receipt of input signals from the all vehicle sensors located throughout each parking facility.
g. The number of detectors and signs shall be determined by the Contractor after a walk through as part of their design documentation.
h. Space-By-Space Vehicle Detection
    At the time of proposal, the Contractor shall provide quantities of equipment, locations and costs for the total hardware, licensing and software needed each category: Space by Space; Row; and Level counting in the garages identified earlier.

Q. Pinhole camera

I. Contractor shall install a pinhole camera in each device so that when a transaction is initiated, a ticket is issued, a credit card is inserted, or the intercom button is pushed, the camera captures an image of the driver of the vehicle.

II. The image shall be associated with the transaction and stored as an integral part of the transaction.

III. Pinhole cameras shall be installed in the following devices:
    a. Entry column
    b. Exit column
    c. Transaction Panel
    d. Automatic Pay Station

R. Intercom System

I. The Contractor shall provide a turn-key intercom system that consists of ten host intercom stations per airport and an integrated microphone and speaker in each Entry Station, Express Exit Station, Transaction Panel, Cashier Station and Employee Parking Pedestal.

II. The intercom shall be a push-button intercom with integrated camera that focuses on driver such that in the event a patron needs assistance while stopped in a lane, the button can be pushed and a connection established between the field location and the host intercom station.

III. In the event that the arming loops are triggered for a configurable amount of time with no transaction being initiated, the intercom station in the lane shall automatically call the Parking Management Office.

IV. The intercom system shall utilize VOIP.

V. The intercom communications shall be directed to a command desk console located in the Parking Management Office (PMO) or Command Center of each airport with roll over capabilities to a second base station as designated by the Port Authority or other telephone/cell phone. The PMO shall be equipped with an intercom base station that displays the physical location of the incoming intercom call. Incoming calls to the base station shall employ visible and audible signals to alert PMO staff.

VI. Once activated, two-way communication shall be possible and the intercom line remains open until the parking staff member terminates the call.

VII. All intercom conversations shall be recorded and stored for a minimum of thirty (30) days.

VIII. It shall be possible that if one intercom is open, and a second call comes in, the attendant shall place the first call on hold and answer the second call.

IX. As part of its Proposal, the Contractor shall submit product data of the intercom base station and push button intercom terminals.

X. The hardware shall have noise filtering capabilities in both the field devices and the central intercom stations.

S. Validation System

I. The PARCS shall create, process, and track multiple forms of fee discounts and validations electronically in the system. Discounts and fee modifications can be related to such items as: Americans with Disabilities Act (ADA), Disabled Veterans, Port Authority developed validations and coupons, etc.

II. The Contractor shall provide an electronic validation system whereby the Port Authority may discount a patron's parking fee by either re-encoding their parking ticket, issuing a magnetically encoded, barcode or QR code voucher, or issuing an electronic barcode or QR code for presentation by a smartphone.

III. Validations shall be made for fee modifications or discounts expressed in specific dollar amounts per transaction or per time period (e.g. $5.00 off total fee or $5 off per day), specific durations of time (e.g. two hours free, one or

more days free, etc.), for the entire parking fee, or a fee calculated at a reduced or alternate rate structure for an individual ticket. Contractor shall provide a method of tracking validations issued by user with a comment field to be completed upon entering the validation.

IV. The Port Authority shall create validations via Validation Stations that are connected to the browser-based PARCS, and protected by username and password. The Contractor shall be responsible to ensure that the validation stations function in accordance with these specifications even if the validation stations are connected to an existing Port Authority computer workstation.

V. Only users with appropriate authorization shall issue validations and the PARCS shall track all validations for auditing purposes by user, validation date, validation type, and validation amount.

VI. Five (5) validation stations shall be provided by the Contractor for each airport, locations to be determined by the Port Authority.

VII. The Contractor shall submit a cut sheet of the proposed Validation Stations as part of its Proposal.

T. Mobile LPI System

I. Contractor shall equip six (6) Port Authority provided vehicles with LPR CCTV cameras and associated computers to record license plate data of vehicles parked within the Port Authority's parking facilities. Where possible, Mobile LPI equipment in these vehicles should be integrated into the vehicles in a modular "plug-and-play" manner so that removal or transfer of the Mobile LPI equipment incurs minimal downtime and modification to the vehicles.

II. The nightly inventory from the Mobile LPI shall be automatically uploaded into the PARCS servers within thirty (30) minutes of completion of the inventory. Upload shall be performed wirelessly from the field. The Contractor shall submit its network requirements to implement this function and TEC will design and build the network infrastructure to accommodate.

III. The Mobile LPI system shall use route-specific software for the inventory taking process, meaning that the inventory takers shall follow a pre-defined route when circulating through the facilities to obtain the inventories. However, because the availability of parking spaces and possible reconfiguration of the parking layouts, the Contractor shall provide a GUI to alter the pre-defined route in order to reflect changed parking configurations. Contractor shall develop the most efficient routing through the Port Authority's parking facility to minimize the amount of time required to capture the nightly LPI.

IV. Vehicles shall be equipped with multiple cameras in order to capture license plate data from vehicles parked on either side of a bi-directional or uni-directional drive aisle.

V. Each Mobile LPI vehicle shall acquire an image of a vehicle's entire license plate at a ninety-five percent (95%) rate for all non-exception vehicles as defined within this section.

VI. Corrections can be performed once the inventory has been uploaded to the server. The image of the plate shall accompany the digital data uploaded. The uploaded data from multiple vehicles shall be merged into the database to form a complete picture of the airport for that day.

VII. The same rules for capturing License Plate Numbers as in the LPR system shall apply for the Mobile LPI system.

VIII. The Contractor shall provide a means, subject to approval by the Port Authority, to remotely test accuracy of the Mobile LPI system to ensure it meets the functional requirements stated herein. The Contractor shall transfer images from each vehicle to a storage format such as CD-ROM, DVD, or uploaded to an FTP site that can then be viewed and its accuracy tested. Port Authority shall select any images stored on the LPR database for scoring purposes. The Contractor shall provide all software needed to test the LPR Subsystem's performance. The software shall be downloadable to a standalone PC used for testing.

U. LPI Manual System

I. The Contractor shall propose a License Plate Inventory (LPI) system to manually capture vehicle LPNs for a LPI database to assist in exception transaction processing and to facilitate customer service activities such as helping patrons locate a lost vehicle. The LPI system shall use route-specific software for the inventory taking process, meaning that the inventory takers shall follow a pre-defined route when circulating through the facilities to obtain the inventories. However, because the availability of parking spaces and possible reconfiguration of the parking layouts, the Contractor shall provide a GUI to alter the pre-defined route in order to reflect changed parking configurations. Only authorized users shall modify routes or data. The PARCS shall modify user access levels to the LPI system.

II. The LPI system shall include all hardware and software for a fully functioning LPI taking and reporting system that is completely and fully reconcilable with the PARCS ticket inventory and the LPR system's active image inventory. The Contractor shall provide an automated, software application to reconcile the LPI inventory and LPR image inventory. The software shall include reconciliation tools, vehicle lookup tools, and LPR/PARCS/PSCS reconciliation software.

III. The LPI system shall accommodate the following tasks:

a. Inventory taking – at specified intervals (e.g. each night), inventory takers shall circulate the parking facilities with handheld devices to record each vehicle's LPN. The LPI shall record by facility, aisle, unique space number, and LPN.

b. Inventory upload – after completing the inventory, the inventory takers shall return the handhelds to a docking station connected to the LPI workstation to upload the nightly inventory. Appropriate checks and balances shall be in-place to detect possible data entry errors.
c. Reconciliation – Upon successful upload and adjustment of the Port Authority-wide inventory, the LPI shall be reconciled with the LPR active inventory. The reconciliation process shall not alter the accuracy of the true number of vehicles parked in a parking facility.
d. Route modification – it shall be possible to add, delete, or modify the inventory routes as well as add or delete entire facilities from the LPI system.
e. The LPI system shall recognize a vehicle that has changed spaces since the last inventory was taken, but that has not exited the facility and re-entered.
f. Nightly upload of data into PARCS and reconciled against LPR data.

IV. LPI Handhelds
a. The Contractor shall provide ten (10) LPI Handhelds per airport to permit simultaneous Manual LPI in each lot with the following capabilities and features:
1) LPN Field that accommodates one to eight characters
2) Automatically recalls the LPN that was parked in each space on the previous night
3) Docking for upload of LPN Inventory
4) Withstands drops from a height of up to four feet on concrete
5) Dust/water/rain resistant to a minimum IP code rating of IP54.
b. As part of its Proposal response, the Contractor shall submit product data of all proposed LPI Handhelds.

V. LPI Workstations
The LPI subsystem shall be accessible from any authorized workstation on the Port Authority network. In addition, the Port Authority shall make available two workstations to be located in each airport's PMO to be designated for LPI. This workstation shall host the docking ports from the handheld devices and serve as the location to perform the nightly LPI/LPR reconciliation.

VI. LPI shall reconcile with PSCS and LPR daily. Daily reconciliation reports shall be generated automatically and emailed to designated recipients for review.

V. Automated Pay Stations

The Contractor shall install Automated Pay Stations (also referred to as "Pay-on-Foot" or POF) as a part of this project.

I. Pay-On-Foots (POFs) shall be installed at approximately one hundred seventy five (175) locations convenient for patron use, to be identified by Authority

personnel. The approximate number of these, which shall handle both credit and cash transactions is forty (40). The Authority may elect to purchase additional devices at any time under this Contract. Pricing shall be based on the prices in the Contractor's pricing sheets, accepted by the Port Authority at Contract commencement, with allowable increases or decreases in accordance with the contract terms.

a. Newark International Airport APS Total: 65
    1) Credit card only: 50
    2) Credit card or cash: 15
b. LaGuardia International Airport APS Total: 40
    1) Credit card only: 30
    2) Credit card or cash: 10
c. JFK International Airport APS Total: 65
    1) Credit card only: 55
    2) Credit card or cash: 10
d. Stewart International Airport APS Total: 5 credit card or cash

II. The Contractor shall provide Automated Pay Stations (APS) devices that are integrated into the PARCS. Actual deployment locations shall be designated by the Authority. The Contractor to provide the Authority with electrical and communications requirements as a part of its proposal for the Automated Pay Station devices and the Authority shall provide all electrical infrastructure and data communication infrastructure to the nearest FOIC to support the POF devices. The Contractor shall be responsible for infrastructure from the FOIC to the POF, installation and configuration of the POFs. In order to accommodate location flexibility, portability and reduce construction and ongoing operating costs, the Contractor shall identify the options and requirements to connect multiple POFs to a single FOIC in a manner that complies with PCI DSS standards and meets Authority approval.

III. All payments made at a POF shall be transmitted in real time to all exit lanes in the appropriate lot or garage whether online to the servers or not. If offline to the servers the data shall still be sent real time to the exit lanes should they be accessible, and subsequently to the servers when communications has been restored.

IV. POF Requirements

a. Credit Card POF features - All POF devices shall provide the following features and functionalities:
    1) Meet all current ADA requirements and standards
    2) Access door with secure vandal proof locking mechanism and no master keys
    3) Equipped with intercom and a pin hole camera that focuses on patron – identical to intercom equipment as provided elsewhere in the PARCS
    4) Visual instructions for patrons to understand the sequence of events to complete a transaction without an understanding of English

5) Color patron interface touch screen monitor
6) Cancel button that allows a patron to cancel a transaction once a parking ticket has been inserted and before any credit card payment made
7) Colors for the pay stations, all text, and graphics shall be configurable and approved by the Port Authority prior to manufacturing
8) The Pinhole camera is to activate at the start of each transaction, regardless of the type of credential (ticket, Smart phone QR, etc.) presented or upon activation of intercom
9) Treated as a Point-of-Sale (POS) and fully integrated into and on-line within the PARCS
10) Utilizes single-slot technology for ticket and credit card insertion and reading where possible
11) Reading both credit cards (EMV chip embedded cards) and magnetic striped credit cards
12) Readers to read either paper or electronic (smartphone) bar code and QR code
13) Twelve key pad for entry of PIN codes
14) Completing on-line, real-time credit card authorization per PARCS specifications on credit card processing.
15) Operate offline when network connectivity is interrupted and incorporate Offline store and forward capabilities for subsequent resubmission when communications restored
16) The grace time (the number of minutes between the time a ticket is paid and the time a driver exits with vehicle through exit lane) shall be parameter driven and with modification by the Authority for each facility and lot. The POF grace time shall also be configurable for each individual POF. There shall be a separate mobile device grace time
17) Each POF shall be able to access the rate tables for all lots and apply applicable discounts based on the LPN and lot associated with the credential supplied
18) Log when a cabinet has been opened or closed; date and time recorded in real-time on the Event Log
19) Receipt generation
    i. Upon successful payment, provide the ability to print a receipt that includes the pay station identification number, facility identification, time and date, fee, amount paid, credential ID (QR or ticket number) and transaction number if requested
    ii. Receipts for credit card transactions shall not display more than the last four digits of the credit card number.
    iii. Receipts for credit card transactions shall be either auto issue or by request. The configurable timeout function for receipt request

shall be set for twenty (20) seconds or until the next ticket is inserted

iv. Create an alarm to display at the Command Center when the receipt paper is low and another non-deletable alarm when receipt paper is exhausted.

20) Shall be configurable to process tickets from select parking facilities and to reject tickets from select parking facilities.

b. Cash/Credit Card POF features - In addition to the requirements above, the cash and credit card POF devices shall provide the following functionalities:

1) Processing parking fee payments using multiple forms of payment, e.g., any combination of cash credit cards, EMV cards, and validations

2) A bank note recycler shall be used. Only bills shall be accepted. The Contractor shall propose the specific make and model of the units to be used along with capacities.

3) At a minimum:

i. A four way bank note recycler which accepts bank note denominations of $1, $5, $10, and $20 in all directions with alarm when recycler is approaching capacity

ii. An alarm for when the recycler is running low. Bank notes dispensed as change shall be in denominations of $1, $5 and $10.

4) All POF Stations accepting cash shall be designed with a note escrow that shall accept and hold the currency until the transaction has either been completed or until the patron has cancelled the transaction and the POF Station has returned the notes.

5) The POF shall not accept a full cancellation if an authorization from the credit card clearing house has been returned for a partial payment and the patron wants to use cash. The POF shall indicate a partial payment accepted and ask for the balance by cash or another credit card.

6) Exiting with a Pre-Paid Ticket - All parking exit lanes shall process tickets that are pre-paid at the POF devices. Exit lanes shall calculate and process the additional fee if the patron has exceeded their grace time for exiting after paying at the POF.

c. Reporting – the PARCS shall contain reports for the POF devices that adhere to the requirements described these Functional Specifications.

d. Contractor shall provide pricing in its proposal for credit card only POF and cash/credit card POF.

W. Automatic Vehicle Identification (AVI) - *E-ZPass® Plus™* and Transponders for Monthly and Employee parking.

I. The functionality to be provided by the *E-ZPass® Plus™* AVI system shall be primarily for accepting *E-ZPass® Plus™* payments from patrons. In addition it

is used as an access control system for Port Authority maintenance vehicles, employees and contractors, certain VIP (Port Authority specified) users, and if selected may be used for select Customer Loyalty Parking Program users to enter and exit the facilities without the requirement for issuing a ticket on entry or reading ticket on exit. The integration shall conform to the Airport Central Host Requirements (see Attachments T and U).

II. The Contractor shall provide a turnkey end-to-end solution that includes the at a minimum, all functionality as currently exists with the following components and services.

III. *E-ZPass® Plus™*

a. The Contractor's proposal must include the equipment and functionality to use a valid *E-ZPass® Plus™* transponder to enter or exit through all lanes, which will be equipped with overhead and patch antennas, and readers, without the requirement to issue a parking ticket at the entry lane or present a parking ticket at the exit lane. (*E-ZPass® Plus™* In and Out). The requirement to not issue a ticket on entry shall be configurable by lane.

b. Accept, parse and distribute daily *E-ZPass®* tag file information to all exit and entry lanes

c. Prepare and send daily revenue data to the *E-ZPass ®Plus™* Customer Services Center (CSC) through an interface as described in the Airport Central Host (ACH) server functional specifications referenced in Attachment T. The Contractor shall identify the method to be used to consolidate the information from all airports for transmission to the CSC

d. Integrate the Airport Central Host server functions into the PARCS.

IV. RFID Transponders

a. The RFID Transponder system functionality shall allow for vehicles using a valid RFID transponder to enter or exit through all lanes, equipped with appropriate readers, without the requirement to issue a parking ticket at the entry lane or present a parking ticket at the exit lane.

b. Integration to the PARCS for customer billing through the Port Authority SAP system for non-public (VIP) and employee parkers. The integration shall conform to the SAP Billing Design Spec v10a and the FDS PANYNJ Parking-Five Star v51 specifications referenced in Attachment T of this RFP.

c. Standardized data transfer processes for integration with the Port Authority's SAP software for monthly parker billing purposes. The system shall provide a text file of all employees marked for billing to the PA's Revenue Control SAP program for billing purposes. The specifications for that file shall be provided upon award.

d. The Contractor must submit, at the time of proposal details for the following:

1) Approach for Installation and commissioning services
2) Mechanism for both Tag and Transaction processing

3) Standard and custom Report generation
4) Selected vendor shall install, integrate, implement, and test the system to ensure components and software performs as required and as designed.
5) Contractor shall provide FCC licensing for all AVI equipment at the time of installation.

e. The AVI Transponder system shall be installed separately from *the E-ZPass®Plus™* system and use transponders that are not based on the *E-ZPass®Plus™* standard.

V. The AVI system shall meet the following minimum specifications:

a. The *E-ZPass® Plus™* system shall ensure that the tag read presented by the reader is the one in the lane. To ensure that is the case and that it is not from an adjacent lane, there are several rules regarding how long the data read shall be held before a primary identification (ticket, QR, etc.) is presented to start the transaction. This is coded into the *E-ZPass® Plus™* readers and is configurable (currently 20 seconds). If an entry identifier is not presented within the 20 seconds the reader shall remove the information. A patch antenna read will then be done. This shall require handing the tag to the cashier or supervisor.
b. The system shall read and accurately identify no less than 99.8% of properly mounted tags that pass through the read-zone.
c. The reader in the AVI system shall provide the data to the POS computer system as soon as it completes the decoding process for the transponder.
d. The AVI system shall process transponder reads at multiple locations, as required, to create a completed transaction. Completed transponder transactions shall be compiled once per day to create actual revenue transactions. Incomplete transponder read transactions, shall be buffered in the system and remain unprocessed until the host computer receives the matching transactions.
e. *E-ZPass® Plus™* transactions shall be completed within a maximum of fifteen (15) seconds.
f. Approved company employees, Port Authority employees, and buses shall utilize the system for ingress and egress to/from dedicated parking facilities. These shall be entered into an Account Management System (see section 9 below).
g. Authorized personnel shall utilize the system for ingress and egress to/from authorized parking facilities as necessary without incurring a fee based on the rules in an Access Management System for each Tag and/or LPN.

VI. RFID Transponders

a. The Contractor shall provide detailed costs for transponders of the eGo long life battery standard based on volumes
b. Transponders shall be of two varieties: Short range for vehicles and long range for buses.

VII. Desktop Reader/Programmer

The Contractor shall provide two (2) desktop reader/writer/programmers with the initial transponder delivery. The desktop reader/programmer shall be provided with all necessary software and hardware to operate the unit using a standard personal computer running Windows.

VIII. Lane System

Each lane system shall operate a stand-alone mode if communications to the Host computer are lost. The equipment in the lane shall be able to store and hold twenty-eight (28) days of transactions, which shall be uploaded to the Host when communications are restored. Additionally, all transactions from the lane are to be transmitted to all other lane/POF equipment associate with the lot.

Each lane system shall maintain a local clock, which shall be synchronized to the Host computer on an hourly basis as a minimum.

Adjustments to the system clock shall not cause errors in the database or system reports.

IX. Software Application

a. The Account management system shall be fully integrated into the parking system in order to provide a seamless access/control system that is fully auditable and provides integrated reports for the parking system as a whole. At a minimum the system shall include all functionality as identified in the current AMS plus any additional requirements created by optional functions listed.
b. The system shall include fully a functional administrative and reporting system that provides the following minimum functions:
    1) Account administration such as:
        i. Open accounts
        ii. Close accounts
        iii. Modify accounts
        iv. Automatic renewal capability if so marked.
        v. Acceptance of import files and ability to export files in predetermined formats
    2) System shall require the following information, at a minimum, to be entered and maintained:
        i. Company name, number, contact information
        ii. Patron name
        iii. Patron’s address
        iv. Email address
        v. Vehicle identification
            a) Make
            b) Model

c) License plate number

vi. Transponder numbers (RFID and/or *E-ZPass® Plus™*

vii. Patron PIN number (if allowed) and *E-ZPass® Plus™* tag number (if used), dates activated, suspended, re-activated

viii. Multiple tags and plates to individuals in an account

ix. Billing indicators – Is this company, patron to be billed

a) Billing rate indicators to be used.

b) SAP - AR account number

c) Unique company account number and name

d) Taxing Authority information: NY, NJ or No tax

X. Report preparation and printing

A complete set of reports is required for tracking the usage of transponders in AMS. Critical reports include monthly usage, monthly billing, listing of all tags in the system per AR account and per Customer account, anti-passback violations, overlapping occupancy for a patron account with multiple vehicles associated to a tag. Other reports in the current system are listed in Attachment I.

The billing report shall match the billing file sent to the SAP system. However, it may also include accounts that are not billed and would not be in the file.

XI. AVI Audit controls

a. The Account management system shall provide full accounting functions including account generation, tracking, invoicing, and account payment collection. Actual invoicing is done through the Authority's SAP system. The Account management system shall be able to prepare records for transmission to that system and include the account numbers required for the SAP system as well as the account number in the system.

b. The system shall control transponders that allow universal access to one, multiple, or all facilities depending on parameters that are input.

c. The Port Authority shall issue and register RFID transponders. *E-ZPass® Plus™* transponders are issued by the various Inter Agency Groups. The Port Authority shall create user groups or categories of AVI transponders.

d. Authorized staff shall manage AVI privileges and access rules in accordance with the security standards for the PARCS. The AVI access system shall provide for expiration of account / AVI transponder for unpaid fees and expirations; also, for lost tags (payments), and if selected imposition of late fees at user-programmable intervals.

e. The system shall report the occupancy of AVI patrons in each facility, in real-time.

f. All user group parameters and rules shall be accessible and changeable by Authorized personnel at the Port Authority via a GUI accessible on any of the PARCS workstations provided with the system. Software code changes shall not be required to edit user group parameters and rules.

g. User groups and individuals within the user groups shall each assign access privileges based upon facility, date, day of week, time of day, length of stay or any combination thereof. For example, it shall be possible to set an employee's access privileges to allow access to the Employee Parking Lot valid only Monday – Friday from 8:00 AM – 5:00 PM or to provide for N hours parking before a fee shall be imposed based on specific rate tables. It shall also be possible to modify user groups or individual accounts to be exempt from anti-passback rules.

XII. Transponder Inventory Management System

a. The Account management system shall provide a transponder inventory management sub-system that shall include the following information, at a minimum:
   1) Total number of transponders in inventory
   2) Active transponders and assignee
   3) Transponders in storage
   4) Lost, stolen, or invalid transponders
b. Authorized users shall maintain the inventory to update the status and quantity of transponders, add or delete transponders, and make other adjustments to the inventory as may be necessary.
c. Full inventory reporting shall be provided to include counts by different transponder types, numbers of failures, mean time between failures and costs.

X. Prebooking and Prepayment

I. Module Requirements

a. Customer Experience
   1) Making an Online Booking
      i. The look and feel of the booking conversation shall match the current look and feel of the current Airport websites and accommodate the different style requirements of the airport websites.
      ii. The booking conversation shall start from either, whichever the customer chooses to use:
         a) the Port Authority home page www.panynj.gov or
         b) the landing page of the customer selected airport
      iii. Any customer wishing to pre-book parking at any of the Port Authority airports shall be taken through the booking conversation in a strictly stepped process.
      iv. Each step except the last one shall be reversible via one click to the previous step to allow easy checking and/or amendment of the booking.
      v. Step 1 – Parking Dates, Times & Airport
         a) The customer shall be presented with a data entry frame positioned on the Port Authority website home page and/or

also on the landing page of their selected airport to start their booking conversation.

b) A 'help' feature for terminal identification is desirable as departure terminal may not be known to the customer. A drop down list of airlines with associated terminals numbers may be one solution.

c) The customer shall be able to
   - either insert their dates/times directly or select the relevant dates/times from active drop down lists and/or drop down calendar pages
   - select the airport they plan to use from a drop down list
   - select the passenger terminal they wish to park closest to
   - insert a promotion code of up to 10 alphanumeric characters
   - click on 'Next' to be taken directly to the next relevant page in the booking conversation or click on 'Manage My Booking' to be taken directly to the relevant page to amend or cancel an existing booking

d) The data entry frame shall
   - include Port Authority specified labels for each of the data entry boxes
   - allow authorized staff to insert, amend and remove high resolution graphical images or text content into the various un-used white spaces in the frame
   - include a button, e.g. 'Search' to commence the booking conversation based on the dates, times and promotion codes entered
   - generate appropriate error messages if any of the mandatory fields are not completed

vi. Step 2 – Parking Product Menu

a) The customer shall be presented with a menu of airport specific parking products based on their entered dates, times, airport, terminal and promotion code data and subject to the rules set by the Port Authority.

b) Each parking product shall
   - be clearly titled
   - be physically and visually separated in the display
   - include a brief description of the product features
   - clearly indicate distance/time and travel mode from the parking lot to the passenger terminals
   - show precisely the full cost of each offering including a clear statement of the savings versus gate price for the same product

- include buttons/links for additional information on parking lots, products and also to display appropriate maps
- include a button for 'Book Now'
- have the capability to include a graphical image
- have the capability to show that a product is sold out for the particular dates requested
- The product menu shall be capable of being presented in an ordered list configurable by authorized trained staff, e.g. to show the products
  - in order of price – highest to lowest, lowest to highest,
  - in order of distance from the terminal - nearest to furthest etc.

c) A button labeled 'Book Now' or equivalent shall be provided opposite or in line with each product to enable customers to select their required parking product and to continue the booking conversation.

vii. Step 3 – Additional Services

a) The customer, having selected his/her preferred parking product, on pressing the appropriate button, shall be taken to a shopping cart page where
   - the details of the selected parking product are set out
     - parking lot identifier – name, number & airport
     - parking lot entry date and time
     - parking lot exit date and time
     - fee payable including taxes and administrative charges
   - at the Port Authority's discretion the customer may be offered a range of
     - add-on services – car cleaning, detailing, servicing, insurance, lounges, fast-track, foreign exchange, retail etc.
     - upgrade offerings - move to a parking lot closer to the terminal for a stated surcharge

b) A button labeled 'Continue' or equivalent shall be provided at the bottom of the page.

viii. Step 4 – Personal Details

a) The customer, having completed the shopping cart process, shall be taken to the personal details page where the details of all of his/her selections are clearly set out and they are invited to provide mandatory personal information including each of the following:
   - first name
   - last name
   - email address – twice

- parking lot access credential details such as License Plate Number or *E-ZPass®* tag number, for example

b) Customers shall then be invited to 'opt out' to a number of Port Authority defined proposals including to
- create an account
- save personal details on the customer's browser and/or
- sign up the airport(s) loyalty club and/or
- receive Port Authority promotional materials via email and/or
- receive Port Authority promotional materials via SMS and/or
- receive booking confirmation by SMS

c) If the customer opts to receive confirmation messages via SMS the system shall immediately prompt them to provide the full cell phone number (twice) to which they want messages sent. Different 'opt-ins' may be required for different options, e.g. SMS messages and marketing emails. Where customers 'opt-in' for a marketing or similar service the solution shall also provide an 'opt-out' feature.

d) A button labeled 'Continue' or equivalent shall be provided at the bottom of the page.

ix. Step 5 – Payment Page

a) The customer, having confirmed their personal details and 'opt in' selections, shall then be taken to the payment page where once again all of the details of his/her product selection(s) shall be set out and his/her personal details summarized.

b) The customer shall be invited to pay for the products using any one of a Port Authority defined set of credit card options – currently Visa, MasterCard, American Express and Discover. The customer shall insert the mandatory credit card information before payment can be processed
- card type – drop down list of accepted cards
- card number (15-19 digits)
- card holder's name as on the card
- security code (shall include 'What is this?' link to a new page with Port Authority defined content and images)
- card expiry date – month and year

c) At this point the system shall include a link to the Port Authority online pre-booking system 'Terms and Conditions' along with a mandatory 'tick box' for customers to confirm that they have read, and to confirm their acceptance of, the terms and conditions.

d) Failure to complete any of the mandatory fields in the required manner shall prompt an appropriate error message and prevent any progress in the booking process.
e) Drop down menus are required, where possible, in each of the mandatory fields.
f) Where applicable, if the credit card used for payment is to be a credential for access to the selected parking lot the details shall be encrypted and retained. The customer may wish to use an alternative bank card for access and, in which case, the details of this second card shall be requested and be recorded/encrypted at this point with a clear message that the second card shall not be charged.
g) A button labeled 'Book and Pay' shall be the last item on the bottom of this page.

x. Step 6 – Confirmation Page
a) On completion of the booking conversation the customer shall be presented with a formal statement of his/her purchases in a booking confirmation page and tax receipt page combined including
- a unique booking reference number – alphanumeric format
- airport name
- booked parking lot arrival date and time
- booked parking lot departure date and time
- booked parking lot
- customer name
- customer email address
- customer credential details
- fee paid
- the issuer name and the last 4 digits of the bank card used to pay
- cell phone number if SMS opt ins are ticked

b) The booking confirmation page shall include summary details of the location of the booked parking lot and the process for accessing the parking lot using the credentials provided during the pre-booking. In addition the confirmation page shall include the capability to offer the customer
- downloadable Port Authority configurable voucher/coupon images and
- the option to participate in a Port Authority definable online customer survey, e.g. via a link to sites such as 'Zoomerang.com'.

c) The booking confirmation page shall include a 'Print' button.

xi. Step 7 – Confirmation Email/SMS
   a) Each customer shall automatically receive a Port Authority definable message specified by him/her in the Personal Details page via
      - email sent to the email address and
      - SMS sent to the cell phone number (optional)

xii. Step 8 – Reminder Email
   a) The proposed solution shall include the option for the Port Authority to ensure that each customer automatically receives a Port Authority definable
      - email sent to the email address provided and/or
      - SMS to the cell phone number provided

      with a summary of the details of the booking at a Port Authority definable period in advance of his/her expected arrival time/date at the parking lot, e.g. 48 or 24 hours.

xiii. Step 9 – Thank You Email
   At the option of the Port Authority, each customer shall automatically receive a Port Authority definable email and/or SMS to his/her email address/cell phone number 24 or 48 hours after his/her booked return date/time to thank the customer for his/her patronage and possibly to offer the opportunity to participate in a customer survey and/or to offer coupons/vouchers/promo codes to pre-book parking on his/her next trip.

2) Other Customer Booking requirements

i. Each page of the booking conversation excluding the confirmation page shall include links to enable the customers to reduce, extend, cancel or amend their booking details by returning to the data entry frame.

ii. Each page of the booking process shall include links or buttons to
   a) a booking management function (see 3.2 below for details)
   b) appropriate airport specific parking lot map images and parking lot information pages
   c) airport specific frequently asked questions (FAQs)
   d) Port Authority specific and airport specific Terms and Conditions
   e) return to parking home page

b. Customer “Manage My Booking” Function

1) The proposed solution shall include the capability for pre-booked customers to re-visit their online bookings at any time prior to arrival at the parking lot, subject to Port Authority controlled restrictions, using at least two (2) unique identifiers, e.g. booking reference

number and their email address. The system shall allow customers with valid open bookings to

i. reduce the duration
ii. extend the duration
iii. amend the entry, exit, parking lot, product, service, credential, contact details or
iv. cancel the booking

2) These functions need to be available at any time prior to their booked time of arrival at their nominated Port Authority parking lot subject to Port Authority selectable/definable rules
3) The amendable fields shall include
   i. expected date and/or time of arrival at the selected Port Authority parking lot
   ii. expected date and/or time of departure from the selected Port Authority parking lot
   iii. email address
   iv. credential details
   v. cell phone number if specified
   vi. parking lot or terminal (subject to change in fee payable)
4) The proposed solution shall enable changes to any or all of these fields in a one step process.
5) In the event the changes result in additional fees being payable to the Port Authority the system shall either
   i. initiate a new payment process for the additional fees before confirmation of the new arrangements or
   ii. effectively cancel and refund the original booking and initiate a new payment process for the total fees payable for the re-configured booking.
6) In the event the changes result in some or all of the fees paid by the customer being repayable to the customer the system shall, if appropriate, automatically initiate a refund process for all fees due to the card account used to make the original booking only, before confirmation of the new arrangements.
7) On completion of the 'Manage My Booking' process an updated confirmation page shall be displayed and an updated confirmation message shall be sent via
   i. email to the email address used to make the original booking and/or
   ii. SMS to the cell phone number specified in the original booking
8) Within the 'Manage My Booking' function customers shall also be able to access, using the identifiers above
   i. a listing of all bookings made via their email address both historic and future bookings and

ii. details of all payment transactions on their credit/debit card account when using the system
iii. details of any modifications made to bookings

c. Customer Access to Promotional and Loyalty Club Offers
   1) The proposed solution shall enable
      i. Authorized and trained Port Authority users to
         a) specify, change, cancel one or more lists of promotion codes (to be single use or multiple use codes) and
         b) link certain categories of promotion code(s) to specified parking lot products and/or parking lot rates and/or parking lots and/or periods/events and/or groups of parking lots including all parking lots at particular airports or to all long term parking lots at any of the four airports that have them.
      ii. Customers who enter a valid promotion code along with their dates/times & airport shall, subject to Port Authority specified rules, be offered the linked promotional offers.
      iii. Customers who hold a membership number of the Loyalty Club on entry of a promotion code and their membership number, be provided with the appropriate linked Port Authority selectable special offers, e.g. air miles or points to be used against future parking or retail purchases at the airports.
   2) Port Authority users shall be able to control and manage the promotion codes and the membership list numbers both manually and via an integrated system interfacing to the appropriate Port Authority system.
   3) The proposed solution shall ideally include a capability, at the Port Authority's discretion, to integrate with third party loyalty programs, e.g. airline air miles programs and national retailer programs in addition to integrating with Port Authority programs. Vendors are invited to set out details and illustrative case studies of existing integrations of this type.

d. Shopping Cart Function
   1) Following selection of their preferred parking product and, at the Port Authority's option, the customers may be offered a range of additional services or trade up offers, e.g.
      i. Airport fast track
      ii. Airport lounges
      iii. Car cleaning, detailing, servicing etc. service
      iv. Airport retail services
      v. Valet parking service
      vi. Upgrade from one parking lot to another
      vii. Insurance coverage for inflexible parking products
      viii. Other value added services provided by the airport or by qualified third party suppliers

2) The Port Authority shall be able to strictly control and manage all and any of these offers.

e. Customer Relationship Management
   1) The proposed solution shall enable the Port Authority to download from the solution database at any time, and in a format suitable for editing and sorting, customer email addresses such that Port Authority can automatically issue promotions and special offers, welcome home, survey, market research, major event notification, e.g. airport or parking lot closure notice to selectable customers as a standard function. The solution shall enable the Port Authority to identify email addresses of customers who have 'opted in' and to exclude all other email addresses from such lists.
   2) The Contractor shall set out details and illustrative case studies of existing integrations of this type.

f. Other Functions
   1) The proposed solution shall include the following functions
      i. Online customer surveys at the end of the booking conversation or as part of a follow-up contact
      ii. Corporate accounts function to accept multiple bookings made with a single bank card or invoice – and incorporating multiple credentials and/or multiple bank cards as identifiers.
      iii. Access to the Port Authority booking engine for Port Authority selected 3rd parties, e.g. airlines, travel agents etc. on Port Authority selectable criteria – prices, products, times/date, airports, parking lots, commission rates
      iv. The Port Authority shall be able to provide single use only promotion codes to customers. Each code shall expire/become invalid immediately upon use.
      v. The Port Authority shall be able to undertake email promotions including a link to discounted tariffs for prescribed dates/times and customer groups
      vi. The 'opt in' tick boxes on the system shall include 'opt ins' for
         a) general Port Authority marketing purposes and separately for
         b) Port Authority SMS message marketing to comply with applicable privacy, data protection policy and legislation.
         c) Opt out function shall also be provided
      vii. The capability to integrate, at no additional cost to the Port Authority, with other parking lot access credential solutions including
         a) pin pad
         b) RFID tags including toll tags and AVI tags
         c) QR/bar code readers
         d) Blue tooth systems including smart beacons
         e) Near field communications devices/technologies

f) Other similar solutions and emerging technologies.

2) Where Contractor systems offer additional features and functionality likely to be of interest to the Port Authority they shall include details with their Proposals.

g. Prebooking and Prepayment Administration and Payment Function

1) The parking products offered at each airport shall be unique to the particular airport and shall be easily identified as such via a coding system for example. Contractors are shall set out and illustrate their proposals to address this requirement.

2) Access to the administration functions shall be strictly controlled with user IDs and password controls with multiple levels of access rights linked directly to the user ID/Password combinations. This function shall include the ability to limit access to information, product set ups, system configurations, reports relating to specific airports.

3) Administration of passwords access levels shall be strictly controlled and be accessible by not more than two Port Authority administrators without specific written authorization to the vendor system support. The successful solution shall include clear audit trails and reporting functions for access privileges. The allocation of access rights shall be highly flexible and easy to administer by authorized staff.

4) The proposed solution shall include the following administrative functions.

i. Only authorized Port Authority staff shall be able to

a) For selected parking lots and/or airports set up new parking products including setting

- product name
- product code
- pricing
- availability
- allocations

b) Amend, suspend or delete for selected parking lots and/or airports any existing parking product or any of the features of any existing product and to have these changes implemented on the system immediately

c) Inspect, amend, extend, check in, close out and/or cancel any current booking on the system without restrictions as to dates, lead times or status, e.g. already in the parking lot

d) Set up new promotion codes for selected parking lots and/or airports – including one use only and multiple use codes – including as alphanumeric codes and to have these changes implemented on the system immediately

e) Amend, suspend or delete any existing promotion codes or any of the features or content of any existing promotion and to have these changes implemented on the system immediately
f) Set up new loyalty club codes/identification numbers for selected parking lots and/or airports – including one use only and multiple use codes – including as alphanumeric codes and to have these changes implemented on the system immediately
g) Amend, suspend or delete any existing loyalty club codes/identification numbers or any of the features or content of any existing loyalty club codes/identification numbers and to have these changes implemented on the system immediately
h) Enable limited access to and/or export of Port Authority specified reports as read/print only, e.g. to allow 3rd parties or agents to check the status of their bookings, account etc. and to print off copies of Port Authority specified reports.
i) Set up, amend, hide, unhide, delete for selected parking lots and/or airports new content for customer pages including all product titles, product descriptions, instructions, FAQs, T&Cs, confirmation page content, confirmation email content
j) Set up, amend, hide/unhide, delete for selected parking lots and/or parking products online customer surveys
k) Install, remove, manage image files for selected parking lots and/or airports for the data entry frame
l) individual products as displayed on the product selection page, e.g. a star with text on a special promotion parking product
m) booking confirmation page, e.g. a retail voucher or competition image
n) Maps including airport and parking lot maps
o) Download specified reports and/or to customize reports and/or to download raw data in a pre-set format for selected parking lots and/or airports
p) Duplicate product set ups for any one parking lot and/or airport into any other parking lot and/or airport and once installed at the second site to adapt and customize the product to meet the specific requirements of the second location without any impact on the product set up at the first location
q) Set grace times for arrival and departure ‘windows’ for each product, some selected products or all products in a suite

r) Make manual refunds to the credit/debit card account used to make a booking of amounts including but not limited to the full fee paid, part of the fee paid, more than the fee paid on an original booking

s) Access to an offline full test site, a mirror image of the online system other than for data files, for the purpose of testing new developments, changes in advance of transfer to the production system

ii. The patron may make an additional payment via the web site or at the exit lane should the prepayment not cover the actual fee for the stay, which could be due to departure the lot later than anticipated by the patron.

5) Parking Product Options

i. The Port Authority requires a very flexible online pre-booking solution. Authorized Port Authority administrators shall be able to design, create, install, configure, amend, delete parking products with ease including, but not limited to:

a) products by location – parking lot, parking area including nested parking lots, virtual and real parking lots

b) products by duration – calendar days, 24-hour days, periods, calendar weeks, weekends, months etc.

c) products by day/date – day of the week, weekend, season, event

d) products by customer group – promo codes, membership number etc.

e) products by service or service provider– valet parking, car wash etc.

f) products by sales channel – in-path airline or travel agent, corporate travel department etc.

ii. The Contractor shall submit with its Proposal how their proposed solution meets and exceeds these requirements.

6) Refund Management

i. The Contractor's solution shall include the ability to offer automatic refunds for bookings cancelled in advance of the booked arrival time (subject to limitations as defined by the Authority). The proposed solution shall include efficient and secure refund management functionality:

a) Refund facilitated with both full amount refunds and partial or excess refunds enabled but only to the card account used to purchase the original booking

b) Customer refund queries – all records shall be efficiently accessible to nominated and authorized Port Authority staff.

c) Refunds – both automatic and manual refunds shall be efficiently accommodated within the system proposed.

ii. A comprehensive and forensic audit trail is required for all payment transactions including refunds.

II. Technical Functionality for Prebooking & Prepayment Module

a. The Port Authority requires that the proposed solution meets all of the following requirements

1) A certified PCI DSS compliant service in full conformity with Port Authority's information security policy [See Attachment O].
2) If the proposed solution is hosted externally to the Port Authority's infrastructure, it shall comply with the requirements and controls stated in the attached Cloud Computing Framework (Attachment W).
3) 24 hour x 7 day availability of all customer facing functions.
4) The provision of discrete customized online parking pre-booking and pre-payment services at all four (4) Port Authority airports in full compliance with the requirements of this RFP.
5) Support services for Port Authority's online parking pre-booking and pre-payment services portfolio including products, prices, availability, functionality, content, integrations and databases, from go live date and into the future.
6) Development services for the upgrade and enhancements of the online parking pre-booking and pre-payment services at the four (4) airports and via the Port Authority website and the landing pages of the individual airports and future extensions and developments of each of these websites.
7) Future proofed solution with demonstrated flexible capability to operate successfully in the rapidly evolving smart phone/web-enabled devices and social media marketplace.
8) Security and isolation of Port Authority information and transactions
9) If a hosted solution is proposed and accepted, the Contractor shall host the Port Authority's online parking pre-booking and pre-payment service
10) Maintenance of the infrastructure required to provide and support this service
11) Monitoring the infrastructure and alerting based as directed by the Port Authority
12) Provision of appropriate resilience consistent with the requirement for 24 hour x 7 day availability and zero downtime for customer facing functions
13) Provision of full system and data backup facilities consistent with the requirement for 24 hour x 7 day availability and zero downtime for customer facing functions
14) Provision and maintenance of IT security aspects of all communications and server infrastructure
15) Provision of logical isolation (at a minimum) and secured access to Port Authority infrastructure

16) Provision of resilient power requirements consistent with the requirement for 24 hour x 7 day availability and zero downtime for customer facing functions
17) Meet required performance criteria including:
    i. 24 hour x 7 day availability to customers i.e. zero downtime
    ii. Ability to complete 500 completed booking transactions per hour scalable to 1,000 per hour
    iii. 5,000 completed booking transactions per any 24 hour period scalable to 10,000 transactions per day
    iv. Online Authorization delays never to exceed 5 seconds and to average less than 2.5 seconds from customer button click to acceptance/rejection
    v. Forensically auditable transaction and change tracking

b. A full offline test site to, at all times, mirror all key areas of the production site/system, including:
    1) technology,
    2) communications,
    3) operating system,
    4) database,
    5) application software,
    6) data,
    7) interfaces etc.

c. The proposed solution shall allow authorized staff to manage and manipulate the products, prices, presentation availability etc. of each of the airports separately without any risk of un-intended 'cross over' or 'contamination' of other airport set-ups or configurations. An adjustment to a product on, e.g. the JFK set-up shall not change the products, prices etc. on any of the other three (3) airport set-ups.

d. Prebooking & Prepayment Module Reporting and Data Analytics Requirements
    1) Schedule of standard reports required for values, volumes, settlements, historic and future
        i. by selectable product or group of products
        ii. by selectable parking lot, category or group of parking lots
        iii. by airport or all airports
        iv. by date
        v. by date range
        vi. by booked duration
        vii. by fee band
        viii. by day of the week
        ix. by selectable periods, e.g. weekends or Mondays to Wednesdays, or weeks
        x. by customer groups
        xi. by sales channel

xii. by service provider, e.g. car wash, valet, etc.
xiii. other as required

2) Bookings
3) Revenues
4) Refunds by period, by card type, by parking lot, by airport
5) Booked arrivals by selectable date, forward, by booked return date
6) No-shows
7) Departures
8) Transaction tracking—searchable by booking reference number or credential, license plate or surname, partial credit or debit card number
9) Agent/service supplier
10) Credit/debit card
11) Cancellations
12) In its Proposal, Proposers shall include details of:
    i. all standard reports available on their systems including sample reports for inspection
    ii. how and by what deadline they propose to meet Port Authority reporting requirements where their standard suite of reports is inadequate in any respect
    iii. data dump function to enable use of a commercial report generator software package to generate new or custom reports.
13) Refund reports shall retain and display the original payment amount and show separately any refund amount and also by whom, via what system any refunds were made - web site, manual etc.
14) Contractors shall submit any data analytics capability in their proposed solution. Contractors shall also illustrate case studies where through integration with third party systems high quality data analytics capabilities have been realized.

e. Scalability—Proposers/Contractors are required to set out exactly how their proposals will accommodate significant increases in:
    1) volumes of transactions at all Port Authority airport parking lots
    2) numbers of parking lots on the system both real and virtual

III. Development Services

a. The Port Authority requires the Contractor to provide development services encompassing full life-cycle delivery (planning, analysis, design, build and test, user acceptance testing, deployment) of new functionality and related technologies (excluding hardware, operating system, network) into the online parking pre-booking and pre-payment service environment covering:
b. Development of additional websites and smart phone apps
c. Enhancement of existing online parking pre-booking and pre-payment service functionality
d. Integration development

e. Database enhancement
f. Additional e-commerce functionality
g. B2B functionality between the Port Authority and 3rd party business partners
h. Secure and controlled development environment and process
i. The technical skill-sets required to achieve these shall be outlined within the Contractor's Proposal.
j. All modifications, changes etc. shall be fully tested on the test system and fully documented before any changes are deployed on the live system.
k. The cost structure and delivery timeline for any Port Authority development services shall be clearly set out in the proposals and handled via the Work Order process outlined in Attachment C1.

Y. Performance Management Dashboard

I. The Contractor shall propose a performance management dashboard that provides summarized reporting features to Port Authority management.
II. The performance management dashboard shall provide management metrics based on the minimum reporting requirements and an operations and maintenance management perspective.
III. As part of the proposal, the Contractor shall provide samples of the Dashboard and the information available for display.
IV. Details of the performance management dashboard, such as the metrics to be used and how they will be displayed, shall be formulated and finalized as part of the system design workshops.

Z. Impound Lot Functionality

I. The Contractor shall provide an Impound Lot Functionality.
   a. Occasionally, the Port Authority will tow a patron's vehicle from a public parking facility to an impound lot.
   b. Upon exit from the public parking facility by the tow truck, the PARCS shall indicate in the parking transaction that this vehicle has been transferred to the impound lot.
   c. Patrons may retrieve their vehicles by making payment at the parking sales office by cash or credit card. All credit card charges shall be processed and authorized by the credit card clearinghouse in real-time.
   d. Port Authority representatives shall access the open transaction by entering the vehicle's license plate number into a workstation that accesses the PARCS database. The PARCS shall display the entry transaction, the transfer transaction, and the total fee due, including the charge for towing the vehicle to the impound lot.
   e. Upon receipt of payment, the PARCS shall close the entire parking transaction and shall print a customer receipt.
II. Handheld device to accept credit card payments
   a. Contractor shall provide a minimum of two (2) handheld devices for credit card payments for each Airport.

b. Handheld devices shall accept the patron's credit card, verify payment through the Port Authority's clearinghouse on a real-time basis and issue a customer receipt reflecting the parking fee due and the payment. Receipt may be emailed to the patron rather than printed.
c. Automatically update the PARCS database to reflect payment of parking fee due and close out the open parking transaction.

III. The PARCS reports shall include payment for all impound lot transactions as a separate line item.

IV. Credit card transactions processed through the handheld computers shall be integrated into the credit card reports prepared by the PARCS.

AA. Asset Management System

An Asset Management System is required with the following functionality as a minimum:

I. A GUI interface for data entry and viewing all screens and reports.

II. Maintaining a complete inventory of all equipment. Note: For the purposes of this section, equipment shall mean: hardware, software, tools and all other components necessary to make the PARCS work regardless of their location.

III. Provide structure and categories for all equipment in a register and at the same time collect, track and report on each piece of equipment. Information held against each item shall be accessible and sortable by virtually any field. Each item in the database can have as many as 1,000 associated fields. Information such as the following is required:

a. Asset details (type, serial number, description, location, barcode, QR code, manufacturer, etc.)
b. Asset type/sub type - unlimited configurable hierarchy
c. Product type
d. Optional - Purchase price, current value
e. Warranty/maintenance/calibration dates
f. Date installed in field
g. Date removed from field
h. Inventory level required
i. Current inventory level
j. Repair history
k. Components (children assets) and attachments
l. Locations – if moveable asset such as Mobile LPI
m. Supplier and maintenance provider if not the primary Contractor
n. Complete history log per item in database
o. Cost centre and ownership
p. User definable fields per item

IV. Tagging so that tools and equipment can be identified either by directly marking the item or applying a non-removable tag. Different options shall be available for marking tools and equipment such as:

a. Barcodes

b. QR Codes
c. Dot Peening
d. RFID
e. NFC

V. Returns—tracking of returns to equipment suppliers shall include the reason(s), dates, frequencies and other details needed to determine if replacement suppliers is required.

VI. Personnel—A means of recording information for each staff member as well as external contractors and subcontractors should be available. This would be used primarily for determining what staff members have which equipment, how long they have had them for, what they are using them for and when they are due back.

VII. Audit and Chain of Custody—an audit trail, which cannot be altered, is desired to provide management with full chain of custody of each piece of equipment from procurement through to disposal.

VIII. Scheduled Maintenance & Inspections—the system shall be able to create Preventative Maintenance schedules weekly, monthly and quarterly, for distribution to the appropriate personnel for execution. The system shall also allow for entering information of the findings of the technicians.

IX. Consumables/Stock—the system should also be able to track consumables and be able to produce alerts when suppliers reach a configurable level. As some consumables will be procured an installed by others, the system shall be able to alert the specified others by email on approaching reordering requirements. The Contractor shall be responsible for all updates to the rules for each consumable shall be made by the Contractor. This function shall include:

a. User defined reorder alerts
b. Audit trail of stock usage
c. Automated process of stock taking ensuring accuracy

X. Reports—simple and detailed reporting with user defined dashboards and alerts, for complete visibility and control by authorized users is required. All reports shall be viewable online and exportable to in PDA, excel and email. The following report descriptions represent, at a minimum, the reporting requirements for preventative and remedial (or emergency) maintenance as well as inventory control for parts replaced.

a. Service Call Register—provides a log of reported problems and resolutions, including comments. Critical date/time stamps are included. For readability, use “green bar” highlighting to allow visual grouping of multiple liens for a single service call. Data for report may be selected by any combination of Service Call Description and Service Call Reporting columns. It is assumed that Problem and Resolution are standardized and recorded using a selection list, and are not free-form.
b. Closed Service Call Register—provides report of key date/time stamps reflecting processing and handling of service calls. Report may select any

combination of Service Call Description, Service Call Reporting, or Service Call Resolution columns. Ranges may be specified as selection criteria for any date field.

c. Closed Service Call Summary—Summarizes service call information by lane, then by lot, and last by entire airport. User may select reporting date/time range for inclusion, as well as lane(s) or lot(s). Summary column calculations may be further filtered by including our excluding Problems, Resolutions, and/or service calls marked "Excluded". Filtering applied to Summary columns shall be prominently displayed at beginning of report.
d. Problem Summary Report—Summarizes problems and solutions within selection period. For each problem, most commonly found and second most commonly found resolutions are reported. Selection criteria include date/time range, lanes, lots, and/or entire airport. User may also indicate Severity Levels as selection criteria, as well as a threshold outage duration and/or time to repair.
e. Referred Service Call Reporting—Reports on status of service calls that have been referred for resolution to higher level staff. Provides details on items in Service Call Register that have a "referral" problem type. Selection criteria include combinations of Service Call(s), Severity, any Service Call Reporting column and Status.
f. Work Order Report—Provides listing of work orders and extra work assignments showing key processing dates, status and cross reference to labor categories and parts required.
g. Inventory Used—Lists parts and counts of key inventory information as well as inflow and outflow of inventory from stock. Data may be selected using date/time ranges (to select reporting period), specific part(s), part wild card and contains, description wild card and contains.
h. Inventory History—Lists stock items, showing each transaction moving item into stock, into service and out of stock. One row for each "cycle" a part enters and exits physical inventory (stock exits when it is transferred to inventory of another airport, is sent out for repair, or is disposed of). Present Status in first row for an item indicates current inventory status with consideration of all cycles for the item. Data may be selected using date/time ranges, specific part(s), part wild card and contains, and description wild card and contains.
i. Uptime Reports—A set of monthly reports (detailed and summary) which shall show details of all reported remedial or emergency calls. The detailed report shall include all calls in the Service Register, show date/time that the call reached the Technician, the time the Technician arrived at site, the problem reported, the problem identified by the Technician, the corrective action taken, the time the Technician corrected the problem and the time the Technician departed. The report shall also show the elapsed time for the call and the applicable contractual Service

Level Agreement times. The summary report shall show by type of problem reported and by problem identified by the Technician, the counts of occurrences and the total of elapsed times for the call. The system shall also have the ability to show this data in a graphical format. The Service Register shall also contain the source of the reported problem and an indication that the problem has been accepted as corrected by said source.

Parking Access and Revenue Control System—Design, Installation & Maintenance

Attachment F
Reference Form

ATTACHMENT F - PROPOSER REFERENCE FORM

Name of Proposer:_____

Please provide a list of references on the firm's performance of similar work within the last five years, including all current contracts. Use additional sheets as necessary.

Include the following information for each reference:

Customer Name:_____
Address:_____
Contact Name and Title:_____
Phone and Fax Numbers of Contact:_____
Contract date(s):_____
Contract cost:_____
Description of work:
_____
_____
_____

Customer Name:_____
Address:_____
Contact Name and Title:_____
Phone and Fax Numbers of Contact:_____
Contract date(s):_____
Contract cost:_____
Description of Work:
_____
_____
_____

Customer Name:_____
Address:_____
Contact Name and Title:_____
Phone and Fax Numbers of Contact:_____
Contract date (s):_____
Contract cost:_____
Description of work:_____

Parking Access and Revenue Control System—Design, Installation & Maintenance

Attachment G
M/WBE Participation Plan

STATEMENT OF SUBCONTRACTOR PAYMENTS

PA3968 / 03-09

M/WBE Participation Report

Instructions for Statement of Subcontractor Payment: To be submitted with every invoice to be used in conjunction with the M/WBE Participation Plan.

Contract/PO No.: _____

Date of Invoice: _____

Contract Title: _____

Committed M/WBE Goals: M _____ W _____

Prime Contractor Name: _____

Contract/PO Amount: _____

Award Date: _____

Completion Date: _____

PA Project Manager: _____

M/WBE Participation to Date: M _____ W _____

Subcontractor's Name	Address & Phone #	Description of Work Performed or Materials Supplied	M/WBE Status	Total Contract Amount Awarded	Total Previous Requests	Amount Paid to Date	Amount of This Request

In connection with the above-captioned contract: I HEREBY DECLARE AND AFFIRM that I am a duly authorized representative of this company, and that the following Minority and Women Business Enterprises have been contracted with and have furnished, or are furnishing and preparing materials for, and have done or are doing labor on the above captioned contract; that there is due and to become due them, respectively, the amounts set opposite their names for materials or labor as stated; and that this is a full, true, and complete statement of all such MBEs/WBEs and of the amounts paid, due, and to become due to them.

Signature	Print Name	Title	Date

Parking Access and Revenue Control System—Design, Installation & Maintenance

Attachment H
Certified Environmentally Preferable Products/Practices

ATTACHMENT H - Certified Environmentally Preferable Products/Practices

Proposer Name: _____Date: _____

In line with the Port Authority's efforts to promote products and practices which reduce our impact on the environment and human health, Proposers are encouraged to provide information regarding their environmentally preferable/sustainable business practices as they relate to this contract wherever possible. Proposers **must** complete this form and submit it with their response, if appropriate. Proposers **must** submit appropriate documentation to support the items for which the Proposer indicates a "Yes" and present this documentation in the proper sequence of this Attachment.

1. <u>Packaging</u>

Has the Proposer implemented any of the following environmental initiatives? **(A checkmark indicates "Yes")**

____ Use of corrugated materials that exceed the EPA recommended post-consumer recycled content

____ Use of other packaging materials that contain recycled content and are recyclable in most local programs

____ Promotes waste prevention and source reduction by reducing the extent of the packaging and/or offering packaging take-back services, or shipping carton return

____ Reduces or eliminates materials which have been bleached with chlorine or chlorine derivatives

____ Eliminates any packaging that may contain polyvinyl chloride (PVC), or polystyrene or heavy metals

If yes, a description of the practices being followed must be included with the submission.

2. <u>Business Practices / Operations / Manufacturing</u>

Does the Proposer engage in practices that serve to reduce or minimize an impact to the environment, including, but not necessarily limited to, the following items? **(A checkmark indicates "Yes")**

____ Recycles materials in the warehouse or other operations

____ Use of alternative fuel vehicles or vehicles equipped with diesel emission control devices for delivery or transportation purposes

____ Use of energy efficient office equipment or signage or the incorporation of green building design elements

____ Use of recycled paper (that meets federal specifications) in their marketing and/or resource materials

____ Other sustainable initiative

If yes, a description of the practices being followed must be included with the submission.

3. <u>Training and Education</u>

Does the Proposer conduct/offer a program to train or inform customers and employees of the environmental benefits of the products to be offered under this contract, and/or does the Proposer conduct environmental training of its own staff?

☐ Yes ☐ No If yes, Proposer must attach a description of the training offered and the specific criteria targeted by the training.

4. <u>Certifications</u>

Has the Proposer or any of its manufacturers and/or subcontractors obtained any of the following product / industry certifications? **(A checkmark indicates "Yes")**

____ ISO 14000 or adopted some other equivalent environmental management system

____ Other industry environmental standards (where applicable), such as the CERES principles, LEED Certification, C2C Protocol, Responsible Care Codes of Practice or other similar standards

____ Third Party product certifications such as Green Seal, Scientific Certification Systems, Smartwood, etc.

If yes, Proposers must attach copies of the certificates obtained.

5. <u>Other Environmental Criteria</u>

Proposers are encouraged to respond to criteria specifically indicated in this RFP as "Management Approach" (and attach the appropriate documentation) to receive consideration in the evaluation.

I hereby certify, under penalty of the law that the above statements are true and correct.

_____ _____Name _____Date

Parking Access and Revenue Control System—Design, Installation & Maintenance

Attachment I
Background of Existing System

ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

Existing PARCS, Features and Functions

The PARCS installed in 2004 incorporates a variety of features and functions. The system added License Plate Recognition (LPR) and Mobile License Plate Inventory (MLPI) among other functional enhancements. Also running over the network are Booth cameras and microphones used for customer service at JFK and LGA currently. EWR has an independent valet system in operation. The current functional features include the following:

- Traversal flow into and out of the lots using loops, Sonic and Optical sensors
- Revenue Accounting
- Audit Controls
- Rate Control w/provisions for Daylight savings time
- LPR and MLPI
- Monthly Parkers
    - The system supports employee parking in designated lots, paid monthly by companies or individuals is required. Rates for payments are configurable by lot, company, type of monthly parker and individual license plate.
- Non-Revenue exits - Automated Vehicle Identification (AVI), Non-coupon, Coupon, proximity tags, reduced rates – Flexible and configurable
- Support for various payment types:
    - Credit card – Mag stripe
    - AVI (*E-ZPass®Plus™* – Kapsch transponders)
    - Cash handling
    - Check, money orders
    - Monthly and over the counter payments for employee parking
- Proximity tags (transponders) for employee parkers and buses
- Occupancy counting and Occupancy on the Web
- Multiple levels of Security, both physical and logical
- Screen savers for POS units in the exit lanes
- Security classifications and levels with high granularity for all users
- Camera systems
- *E-ZPass® Plus™*
  The PA uses *E-ZPass®* for tolls at various tunnels and bridges and the PARC system uses *E-ZPass® Plus™* for parking as a payment method. *E-ZPass®* and *E-ZPass® Plus™* are a radio-frequency identification (RFID) based system. Currently the PARC system accepts approximately 40% of all transactions from exit lanes by *E-ZPass® Plus™.*

Employee Parking

Employees parking in employee lots are provided proximity tags for entry and exit. In public lots, a VIP process is employed and the patron's license plate is tied to a personal identification number (PIN) or *E-ZPass® Plus™* tag number which will permit exit.

ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

The current system interfaces with the PA revenue accounting department. A flat payment file is created monthly for a Port Authority system for billing to employers for monthly parkers. The current system needs to be expanded upon to provide additional functionality and flexibility for rates.

Available locations for making payment:

- Exit Lanes – Point of Sale (POS) units
- POF (Pay on Foot) Merli Machines – credit card only
- Sales Offices
- Valet Office
- Internet via ABM

Non-Revenue

PA vehicles, certain contractors, and certain employees are able to exit a public lot with no or reduced payments. The rate tables for the lots must be able to accommodate an unlimited variety of rates and conditions.

Reservation System

The reservation system is operated through a website administered by ABM. Currently, payments are accepted by ABM for reservations only and not parking fees.

Valet Parking

EWR has an independent valet system in operation. The valet system can track, monitor, control and manage: valet keys, vehicles, tickets, employees, payroll and revenue. The valet system incorporates the following equipment and functionalities:

Exceptions

The PARCS has the ability to support exceptions such as illegal backouts, tailgating, snow day discounts, emergency exits, etc.

Database

Microsoft SQL and Oracle are the two approved databases in the PA standards. PA currently uses Oracle and a NETAPP appliance to store the data. The system must ensure that no data will be lost and that in the event of a database failure the system will be able to continue uninterrupted operation.

Thirteen (13) months of online data and seven (7) years of archived data are required. Backups and archiving must be done without interruption to online processing and data storage.

All entry lanes, exit lanes and POF's maintain a database which allows them to operate in the event of database or network issues. Once the issue is corrected, the lane and POF units will upload the transactions to the server. Lane equipment and POF units must store at least six (6) weeks of data and have the ability to export that data to an external drive. Lane equipment and POF units also maintain a journal of all activity (eJournal) which is uploaded daily.

Network

ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

The PA has a high speed OC192 backbone fiber network installed at each airport (except SWF). This is a high speed Internet Protocol (IP) network. The current system connects to the plazas in all lots, all POFs, servers, application computers, and to outside systems with either copper or fiber. The new system will use this network. The PA supports the backbone network and the vendor will support all other network components for lots, POFs, valet, etc. on the system.

Booth Intercoms (inside the booth and external for patrons in exits, entries and POF's) are IP based half-duplex (Full Duplex is preferred).

Credit Card Processing
MC/Visa/Discover cards are processed through First Data Services (FDS) to Bank of America Merchant Services North Platform via a Secure Sockets Layer (SSL). American Express is sent directly to AMEX via SSL. Settlement now is SFTP (SFTP is the widely used protocol for transferring information securely)with AMEX and SSL with FDS where all transactions are batched and resent nightly. The system must use host based credit card processing to eliminate the retransmission of the data and simplify PCI-DSS compliance.

Internet
The PA provides all Internet connectivity through its firewalls. Access to the internet is through a gateway router located at each airport.

PA Website
The Port Authority maintains a website for airport parking (http://www.panynj.gov/airports/airport-parking.cfm). The website displays information about parking pricing and real-time lot occupancy rates. Lot occupancy percentages are sent every 5 minutes to the PA website and to Transcom (for 511NY and 511NJ) display.

The PA website does not currently handle online payments.

License Plate Recognition (LPR)
The current system uses License Plate Recognition (LPR) cameras in all exit and entry lanes. Infrared camera is used for LPR processing and closed-circuit television (CCTV) cameras for image capture. Some lanes incorporate the two image features into one camera with an embedded controller. Entry lanes are now post capture and exit lanes are pre-capture. In the new installation, extra lanes shall be installed as pre-capture where possible, and standard reports will contain images of vehicles on entry that backout of the lane with or without the ticket.

Mobile License Plate Inventory (MLPI)
The system currently uses a Mobile License Plate Inventory (MLPI) capture system. MLPI captures all vehicle inventory in the lots each night and uploads the inventory data to the servers. 100% accuracy of plate reads is required. Manual corrections are performed during the capture phase.

Reporting
The current system provides a significant number of canned reports using Business Objects. ad hoc reporting is available for authorized users. See below for a sample list of existing reports for specific report titles.

ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

PARCS Parking Transaction Processing Narrative

PARCS is implemented as a distributed, server-based system designed to optimize system responsiveness, reliability, and expandability. The ONYX host application resides on a robust Sun Solaris V440 Network Server that supports fail-over redundancy to the Secondary Host Computer located in another building on airport property. Both Primary and Secondary Host servers include:

1) Sun Solaris OS
2) Veritas Foundation Suite (facilitates the mirroring of data)
3) BEA Web Logic Application Server
4) HP Open View Network Node Manager

PARCS encompasses the utilization of the Port Authority's existing Oracle licenses. PARCS uses the Oracle 9i database manager and Oracle Application Server for account management.

Both Primary and Secondary Host servers are redundantly connected to the SONET backbone through two Cisco Catalyst 3550 Multilayer Gigabit Ethernet switches, with each switch having two LX single mode GB fiber cables connected to available ports on the existing SONET node.

Common to both ONYX Host servers is the Network Appliance (NETAP) FAS270, providing 8x144 Gb 10k RPM disk drives. Transaction information from the system, including revenue data and optional LPR and CCTV images are stored in a real-time environment providing fast and efficient access to authorized users. The Quantum Tape Drive provides off-site storage of critical system data. Secured access outside of the Port Authority's network is provided through the PA's Firewalls.

A separate report server is employed at the Primary server location to offload the reporting demand from the ONYX Host server and the real-time storage array. The PARCS includes Business Objects Reporter, a reporting tool capable of generating a wide range of reports and report styles. Other Commercial Off The Shelf (COTS) reporting tools may be utilized including Crystal Report Writer.

Connectivity between the lane equipment and the SONET backbone is accomplished through a set of network switches. The lane equipment is concentrated through a D-Link DGS 1008D local switch providing 10/100/1000 BaseT bandwidth to the Cisco Catalyst 3550 area switch.

All lanes and POFs are connected to an applicable Cisco Catalyst 3550 area switch located in a Fiber Optic Interface Cabinet (FOIC) or communications room with connectivity to an available SONET backbone node.

A web-based central management services allow authorized users to configure, control and audit the entire PARCS from secure workstations distributed throughout the facility or from remote locations using any compatible web browser.

Administrators can set fee calculation and access rules based on a variety of criteria, such as patron identification or category of vehicle. Supervisors can monitor lane activity via the web-based CCTV video streams included with LPR processing that are available on-demand throughout the system.

In the lane, Ethernet connectivity exists between the devices and Sapphire Lane Controller controlling access in conformance with centrally managed rules.

Lane devices such as the Cashier Terminal, the Ticket Issuing Device (TID) and the PosiDRIVE 50 barrier gate support vehicle and patron identification using a variety of technologies including magnetic stripe tickets and cards, credit and debit cards, LPR and integrated AVI.

Fully configured with LPR and AVI, PARCS insures that the patron's Primary ID (e.g. ticket, AVI, credit card) and the vehicle in which the patron entered are continuously synchronized throughout the patron's stay in the facility. Traversal data including the traversal time, license plate image and vehicle image are maintained at ONYX and related to both the Primary ID and the license plate number.

Upon exiting the facility, the traversal history is independently retrieved by both the Primary ID and license plate number. Traversal inconsistencies are identified and flagged with automatic notification to the cashier, operations personnel, security personnel or other authorized users. Typical areas of revenue loss are mitigated including ticket swapping, license plate swapping, lost ticket claims and gate crashes.

On exit, currently two forms of identification are required to complete a transaction (with the exception of employee lots, which rely on a proximity card). The first form of identification is the ticket and the second the license plate. *E-ZPass® Plus™* customers entered into the Monthly Parker database, a Valid *E-ZPass®* Tag serves as the first form of identification.

PARCS offers increased security as LPR technology provides a "black" list which can be used for information only or to deny access and payment options.

Existing Communications

The existing PARCS consists of entry and exit lane controls communicating via serial and Ethernet to a network switch in each lane which aggregates to a fiber optic network switch at each plaza. The network switches at each plaza are then connected via fiber optic cable to a node on an OCE-192 SONET ring which serves as the network backbone. Each airport (except Stewart) has their own OCE-192 ring.

Stewart Airport has a communication topology that varies significantly from the above described networks. The Port Authority shall provide a new IP based network for Stewart Airport which shall have connectivity to Port Authority data centers.

The primary and backup servers reside in different locations at each airport and are connected to the OCE-192 ring.

ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

Existing PARCS Lane Equipment

Part Number	Description	LGA	JFK	EWR	Total	Comments/SRO
11-3914	Pushbutton Lightbulbs	56	158	118	**332**	
01-40008	Sonet Node 10/100 Ethernet card	0	0	0	**0**	**Not used anymore**
10-25312	Cable - harness,button light-tid and act	33	79	59	**171**	
10-25315	Display/IR Cable	33	79	59	**171**	
10-25346	Cable - Ticket Dispensor / POF	13	33	23	**69**	
10-25348	cable td400 display cable for TID	13	33	23	**69**	
10-26252	Cash Drawer Cables	40	92	72	**204**	
11-0003	T Handle lock w/key	33	79	59	**171**	
11-11307	24vdc fan cover	33	79	59	**171**	
11-11785	24VDC Fan	33	79	59	**171**	
11-12262	Ultra Sonic Safety Sensor	35	79	59	**173**	
11-1743	5 amp fuses	47	91	72	**210**	
11-25027	Lock Assembly spitter doors	26	66	46	**138**	
11-25159	Patron Credit Card Reader (ACT)	34	58	49	**141**	
11-25178	Check Combo Reader	20	46	36	**102**	
11-25180	ACT Printer (Ithaca)	20	46	36	**102**	
11-25202	ELO Touchscreen	20	46	36	**102**	
11-25224	Cash Drawer	40	92	72	**204**	
11-25258	Sun keyboard type 6	20	46	36	**102**	
11-25489	DB9 terminal adapter, 1 req'd per P357 trigger input	33	79	59	**171**	
11-25510	Fuse Posi Drive Gate	40	86	70	**196**	
11-25511	Gate fuse holder	40	86	70	**196**	
11-25582	Floodlight 45W halogen	33	79	59	**171**	

ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

Part Number	Description	LGA	JFK	EWR	Total	Comments/SRO
11-25583	Floodlight fixture, dual				**0**	**depends on lane configuration**
11-25681	check combo rdr cable	13	46	36	**95**	
11-25803	Sapphire, PANYNJ, configured w/sftwr & drivers	54	98	83	**235**	
11-25839	Novus 2 UPS w/extd alarm card (may run from adj. lane UPS)	40	86	70	**196**	
11-25844	Pin pad (ACT)	20	46	36	**102**	
11-25879	Cisco Switch	14	23	20	**57**	
11-25926	Filters	20	46	36	**102**	
11-25982	Null modem adapter	20	46	36	**102**	
11-25989	Check/combo rrdr power supply	20	46	36	**102**	
11-26011	Cat5 patchcord, 2 meter	378	686	581	**1645**	
11-26099	16 Port Dlink Switches	54	98	83	**235**	
11-26185	Perle (EZ Pass)	20	46	36	**102**	
11-26377	POF MONITOR	14	12	13	**39**	
12-10417	Universal Power Supply	33	79	59	**171**	
12-10424	Comm Gateway Controller	34	58	49	**141**	
12-10438	In-booth Mag Stripe Ticket Reader	20	46	36	**102**	
12-10439	RB Intercom w/outdoor quad box	49	91	72	**212**	
Radio Shack	DB9-RJ12 Connector	20	46	36	**102**	
12-10451	DB9F to RJ45 adapter, 1 req'd per VMS	27	53	47	**127**	
12-10453	HID READ HEAD	7	7	11	**25**	
12-25268	LPR/CCTV post w/L-bracket, U bolt, & (3) 4" caps	60	120	90	**270**	**Estimate**

ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

Part Number	Description	LGA	JFK	EWR	Total	Comments/SRO
20-11903	Main Shaft Crank	40	86	70	**196**	**Included in complete gate count**
20-11907	Motor Crank (Posidrive gate)	40	86	70	**196**	**Included in complete gate count**
20-11922	main spring pivot bar	40	86	70	**196**	**Included in complete gate count**
20-11924	Gate Spring	40	86	70	**196**	**Included in complete gate count**
20-12186	Red reflective tape	40	86	70	**196**	**On gate arm**
20-3469	Gate Warning labels	40	86	70	**196**	**included in complete gate count**
21-11921	Bearing Spring Crank	40	86	70	**196**	**included in complete gate count**
21-11944	Posi Gate Switch (door)	40	86	70	**196**	**included in complete gate count**
30-22073	Patron CC rdr cable	34	58	49	**141**	
30-25976	Retracted Ticket Bins	20	52	36	**108**	
30-26419	exit transport deflector	20	46	36	**102**	
30-26478	ACT cabinet tabs	20	46	36	**102**	
32-22361	TD420 Controller	54	98	83	**235**	
32-22362	TD400 Field I/O Assembly	47	77	70	**194**	
32-22364	Exit Transport (verifier)	20	46	36	**102**	
32-22365	TD 420 Transport Assembly (Dispenser)	13	33	23	**69**	
32-22408	POF Transport	14	12	14	**40**	
32-25207	Issuing Device	13	33	23	**69**	
32-25208	Center stripe ASCOM module	0	0	0	**0**	**Not used anymore**
41-17102	Power Supplies (ACT)	20	46	36	**102**	
41-25652	Receipt Buttons	20	46	36	**102**	
42-16866	POF reciept printer	14	12	13	**39**	
50-14048	Warning Label	40	86	70	**196**	**Included in complete gate count**
50-25072	Connecting Rod (Narrow)	40	86	70	**196**	**Included in complete gate count**
50-25101	Gate Arm end cap	80	172	140	**392**	

ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

Part Number	Description	LGA	JFK	EWR	Total	Comments/SRO
50-25102	Gate Anti-Slip Insert	40	86	70	**196**	**Included in complete gate count**
50-25112	Gate Arms 10ft	40	86	70	**196**	**Included in complete gate count**
51-25110	Gate Motors (Bodine DC motor)	40	86	70	**196**	**Included in complete gate count**
52-14053	LCD Display Interface	47	91	70	**208**	
52-14056	Posi Drive Controller	40	86	70	**196**	**Included in complete gate count**
52-14087	BRO-1 Buffer relay pkg (R/G light control)	40	86	70	**196**	**Included in complete gate count**
53-14001	Gate Drive Assembly (complete - motor,power supply and mech)	40	86	70	**196**	**Included in complete gate count**
53-14073Y	Complete Gate	40	86	70	**196**	
60-26063	Prox intercom mtg plate	7	7	11	**25**	
62-15672	IP Dongles	162	294	249	**705**	**Estimate**
63-15732	HID MaxiProx reader w/Non-metallic Jbox, 8x8x4	7	7	11	**25**	
80-20491	Push for ticket Buttons	13	33	23	**69**	
80-20492	Cancel Buttons	20	46	36	**102**	
80-22386	cable -Display cable ACT	20	46	36	**102**	
80-22387	pin pad cable	20	46	36	**102**	
80-22388	cable - TD400 mag cable	33	79	59	**171**	
80-22391	patron receipt printer cable	34	58	49	**141**	
80-25356	40 pin ribbon cable I/O to td-400 controller	33	79	59	**171**	
82-20059	LCD - Display	33	79	59	**171**	
82-22078	ACT fan filter w/cover	20	46	36	**102**	
82-22383	Receipt Printer (Patron)	34	58	49	**141**	

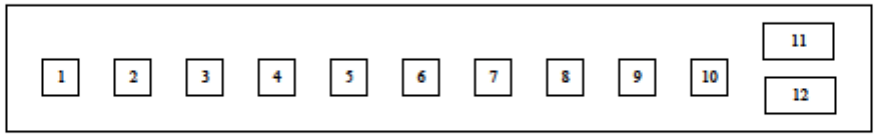
ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

Part Number	Description	LGA	JFK	EWR	Total	Comments/SRO
87-19688	52 pin ribbon cable -(ACT) td400 to transport)	13	33	23	**69**	
CCTV-0004	Spectralite outdoor PTZ color camera	33	79	59	**171**	
CCTV-0006	Spectra outdoor wall pendant w/PS	33	79	59	**171**	
CCTV-0009	Video server, Axis 2400+	21	46	34	**101**	
LPR-0001	P357 Image processor, PANYNJ (PIPs Server)	14	25	18	**57**	
LPR-0004	LPR camera connector	33	79	59	**171**	
LPR-0005	LPR Optical Trigger	33	79	59	**171**	
LPR-0036	Sgl Lane Optical Trigger/Reflector assm w/stands				**0**	
LPR-0044	LPR P356 camera w/swivel brackets & mtg hardware	33	79	59	**171**	
LPR-0045	P356 LPR 810nm camera w/5-50 varifocal lens, long hood	33	79	59	**171**	
LPR-0062	Dual Lane Optical Trigger PVC enclosure upgrade	21	79	59	**159**	
NPN	EzPass patch reader mushroom cap (green)	20	46	36	**102**	
NPN	adj thermostat	13	33	23	**69**	
79	gate motor keys	79	86	70	**235**	
NPN	Photo Cell	33	79	59	**171**	
NPN	CCTV Camera Domes	33	79	59	**171**	
VMS-0019	VMS 1226-2 wall mtd 1.5" char. 2 line Red LED sign	27	53	47	**127**	
VMS-0020	VMS mtg bracket, PA version w/clamps & mtg hardware	27	53	47	**127**	

ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

EWR Switch Layout

EWR



TOP Switch EWRPDC-1
10.100.1.5

1 – NAS Head 1 NIC A
2 – NAS Head 2 NIC B
3 – 10.100.4.2 (WS LAN)
4 – ewrappsp1 NIC 0
5 – VOIP (.233)
6 – ewrdbsp1 NIC 0
7 – ewrdbsp1 NIC 4
8 – ewrrepp1 NIC 1
9 – EWRPDC-2 NIC 9
10 – Ascom 208.206.24.X
11 – Unused
12 – EWRBDC-1 Port 11

Top Switch EWRBDC-2
10.100.1.3

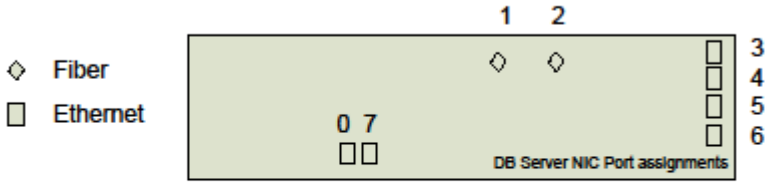
1 – SNMP - OpenNMS
2 – Syslog Server
3 – APC UPS
4 – ewrappsf1 NIC 1
5 – Intellect SONET
6 – ewrappsf1 ALOM
7 – ewrdbsf1 NIC 3
8 – ewrdbsf1 HB2 NIC 6
9 – EWRBDC-1 NIC 9
10 – ewrrepsf1 NIC 2
11 – Unused
12 – EWRPDC-2 Port 12

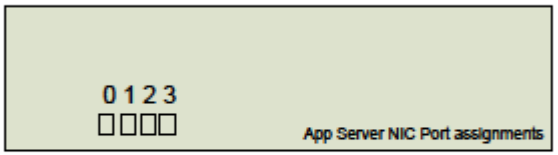
Bottom Switch EWRPDC-2
10.100.1.4

1 – NAS Head 1 NIC B
2 – NAS Head 2 NIC A
3 – ewrappsp1 NIC 1
4 – ewrappsp1 ALOM
5 – ewrdbsp1 ALOM
6 – ewrdbsp1 NIC 5
7 – ewrdbsp1 NIC 3
8 – ewrrepp1 NIC 2
9 – EWRPDC-1 NIC 9
10 – ewrdbsp1 HB NIC 6
11 – Cisco OC192 SONET
12 – EWRBDC-2 Port 12

Bottom Switch EWRBDC-1
10.100.1.2

1 – Unused
2 – Unused
3 – ewrappsf1 NIC 0
4 – ewrappsf1 NIC 2
5 – ewrdbsf1 ALOM
6 – ewrdbsf1 NIC 0
7 – ewrdbsf1 HB1 NIC 4
8 – Unused
9 – EWRBDC-2 NIC 9
10 – ewrrepsf1 NIC 1
11 – EWRPDC-1 HB NIC 12
12 – Cisco OC192 SONET

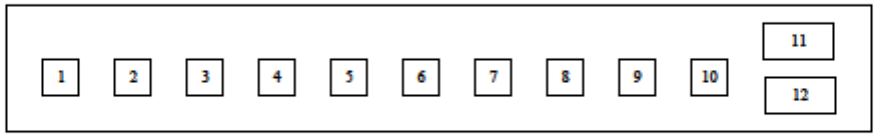




FEDERAL APD Federal Signal Corporation	TITLE Port Authority Development Environment			DESCRIPTION EWR Switch Layout
	PAGE 1 OF 1	REVISED 6/3/2009	Proprietary and Confidential	DRAWN BY Robert Sikogstad	FILENAME Architecture EWR Switch Layout.vsd

ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

JFK Switch Layout



JFK-14-TOP1
10.100.129.3

1 – jfknassp1 NIC A H-1
2 – jfknassf1 NIC B H-2
3 – jfkappsp1 NIC 0
4 – JFK VOIP Srvr
5 – jfkdbsp1 NIC 5
6 – jfkdbsp1 NIC 0
7 – jfkappsp1 ALOM
8 – jfkrepp1 NIC 1
9 – JFK-14-BOT1 NIC 9
10 – jfkdbsp1 NIC 6 (HB)
11 – PAWANet
12 – JFK-145-TOP1 NIC 12

JFK-145-TOP1
10.100.129.5

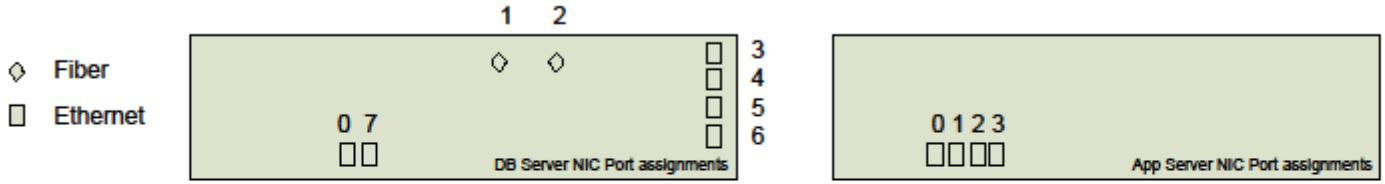
1 – Ascom (208.206.26.X)
2 – jfkappsf1 ALOM
3 – jfkdbsf1 – NIC 5
4 – jfkrepsf1 – NIC 1
5 – jfkappsf1 – NIC 0
6 – jfkdbsf1 – NIC 0
7 – jfkdbsf1 – NIC 4
8 – jfkappsf1 – NIC 2
9 – Interconnect
10 – jfkdbsf1 – NIC 6 (HB)
11 – Unused
12 – JFK-14-TOP1

JFK-14-BOT1
10.100.129.4

1 – jfknassp1 NIC B H-1
2 – jfknassf1 NIC A H-2
3 – SONET OC192
4 – jfkdbsp1 ALOM
5 – PAWANet (VLAN 133)
6 – jfkappsp1 NIC 1
7 – jfkdbsp1 NIC 3
8 – jfkrepp1 NIC 2
9 – JFK-14-TOP1 NIC 9
10 – Workstations (132.0)
11 – JFK-145-BOT1 NIC 11 (HB)
12 – jfkdbsp1 NIC 1 (HB)

JFK-145-BOT1
10.100.129.2

1 – Workstations (132.0)
2 – jfkdbsf1 ALOM
3 – SONET OC192
4 – jfkrepsf1 – NIC 2
5 – jfkappsf1 – NIC 1
6 – jfkdbsf1 – NIC 7
7 – jfkdbsf1 – NIC 3
8 – jfkappsf1 – NIC 3
9 – Interconnect
10 – Intellect SONET OC3
11 – JFK-14-BOT1
12 – jfkdbsf1 – NIC 1 (HB)

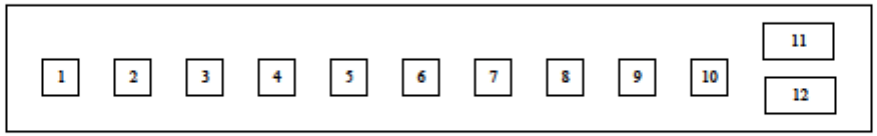


FEDERAL APD Federal Signal Corporation	TITLE Port Authority Production Environment			DESCRIPTION JFK Switch Layout
PAGE 1 OF 1	REVISED 06/18/10	Proprietary and Confidential	UPDATED BY ROBERT SKOGSTAD	FILENAME Architecture – JFK Switch Layout.vsd

ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

LGA Switch Layout

LGA



LGAPDC-B
10.100.65.2

1 – lganassp1 NIC B H-1
2 – lganassf1 NIC A H-2
3 – lgaappsp1 NIC 1
4 – VOIP Server
5 – lgarepp1 NIC 2
6 – lgadbsp1 NIC 3
7 – lgaappsp1 ALOM
8 – lgadbsp1 NIC 5
9 – LGAPDC-A NIC 9
10 – Workstations (68.X)
11 – LGABDC-B NIC 12
12 – lgadbsp1 NIC 1(F) (HB)

LGABDC-A
10.100.65.3

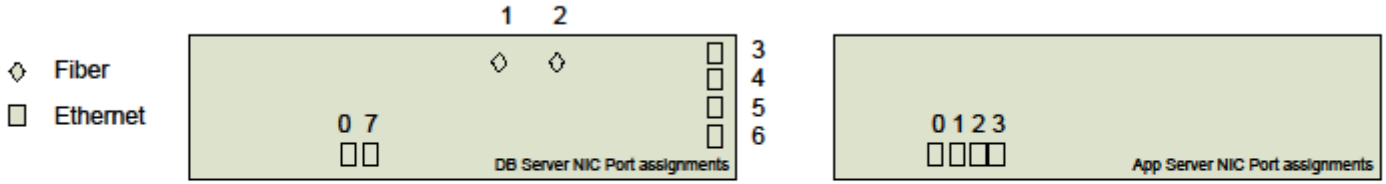
1 – lgaappsf1 ALOM
2 – Syslog Server
3 – lgaappsf1 – NIC 0
4 – lgaappsf1 – NIC 2
5 – lgarepsf1 – NIC 1
6 – lgadbsf1 – NIC 0
7 – lgadbsf1 – NIC 4
8 – lgadbsf1 – NIC 6 (HB)
9 – LGABDC-B NIC 9
10 – Workstations (68.X)
11 – Unused
12 – LGAPDC-A NIC 11

LGAPDC-A
10.100.65.5

1 – lganassp1 NIC A
2 – lganassf1 NIC B
3 – lgaappsp1 NIC 0
4 – lgaappsp1 ALOM
5 – lgarepp2 NIC 1
6 – lgadbsp1 ALOM
7 – lgadbsp1 NIC 4 (HB)
8 – lgadbsp1 NIC 6
9 – LGAPDC-B NIC 9
10 – PAWANet (10.100.69.1)
11 – LGABDC-A NIC 12
12 – SONET OC192

LGABDC-B
10.100.65.4

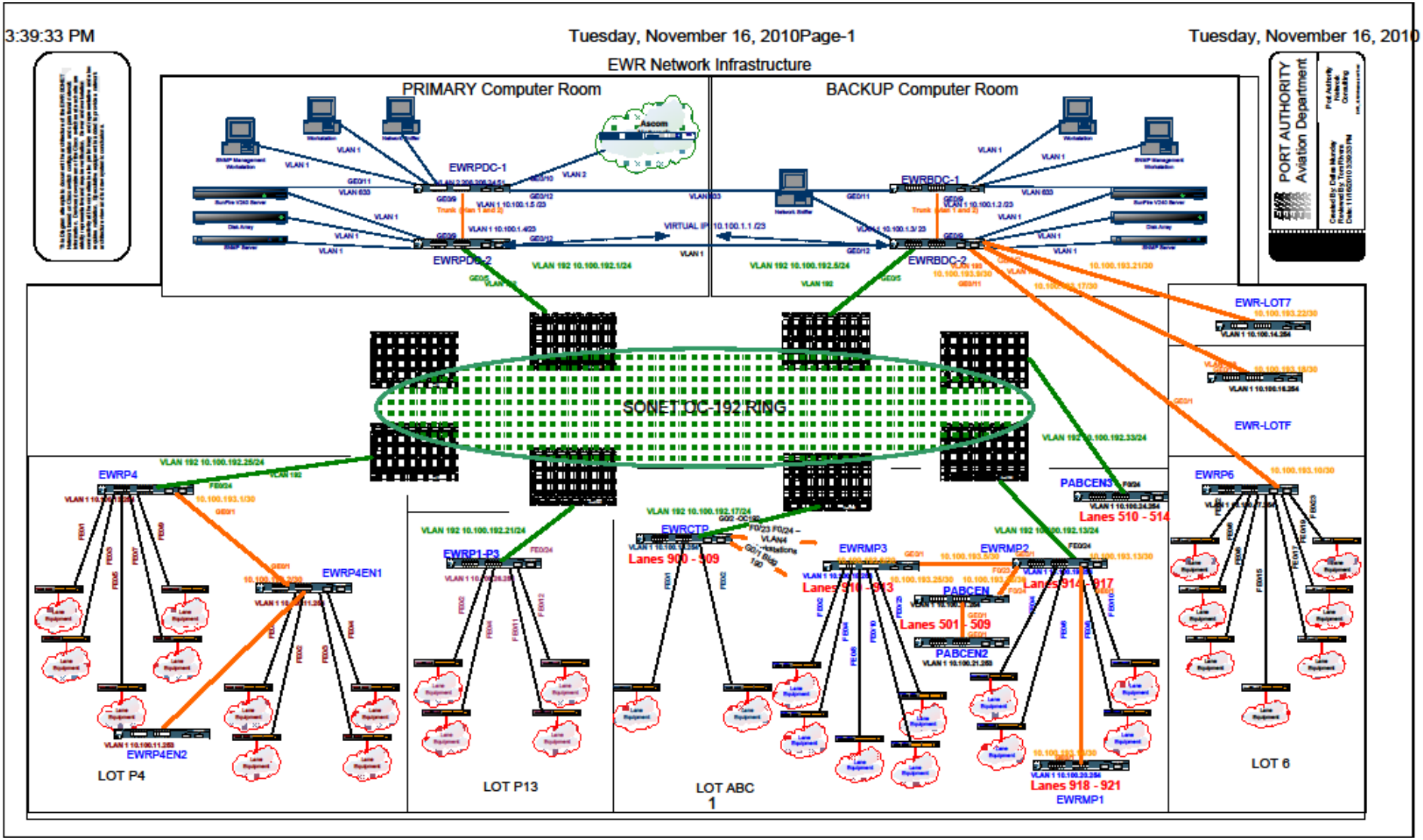
1 – lgadbsf1 ALOM
2 – Unused
3 – lgaappsf1 – NIC 1
4 – lgaappsf1 – NIC 3
5 – lgarepsf1 – NIC 2
6 – lgadbsf1 – NIC 3
7 – lgadbsf1 – NIC 7
8 – Unused
9 – LGABDC-A NIC 9
10 – Unused
11 – lgadbsf1 – NIC 1 (HB)
12 – LGAPDC-B – NIC 11



FEDERAL APD Federal Signal Corporation	TITLE Port Authority Development Environment			DESCRIPTION LGA Switch Layout
	PAGE 1 OF 1	REVISED 07/08/10	Proprietary and Confidential	DRAWN BY Mark Honomichl	FILENAME Architecture – LGA Switch Layout.vsd

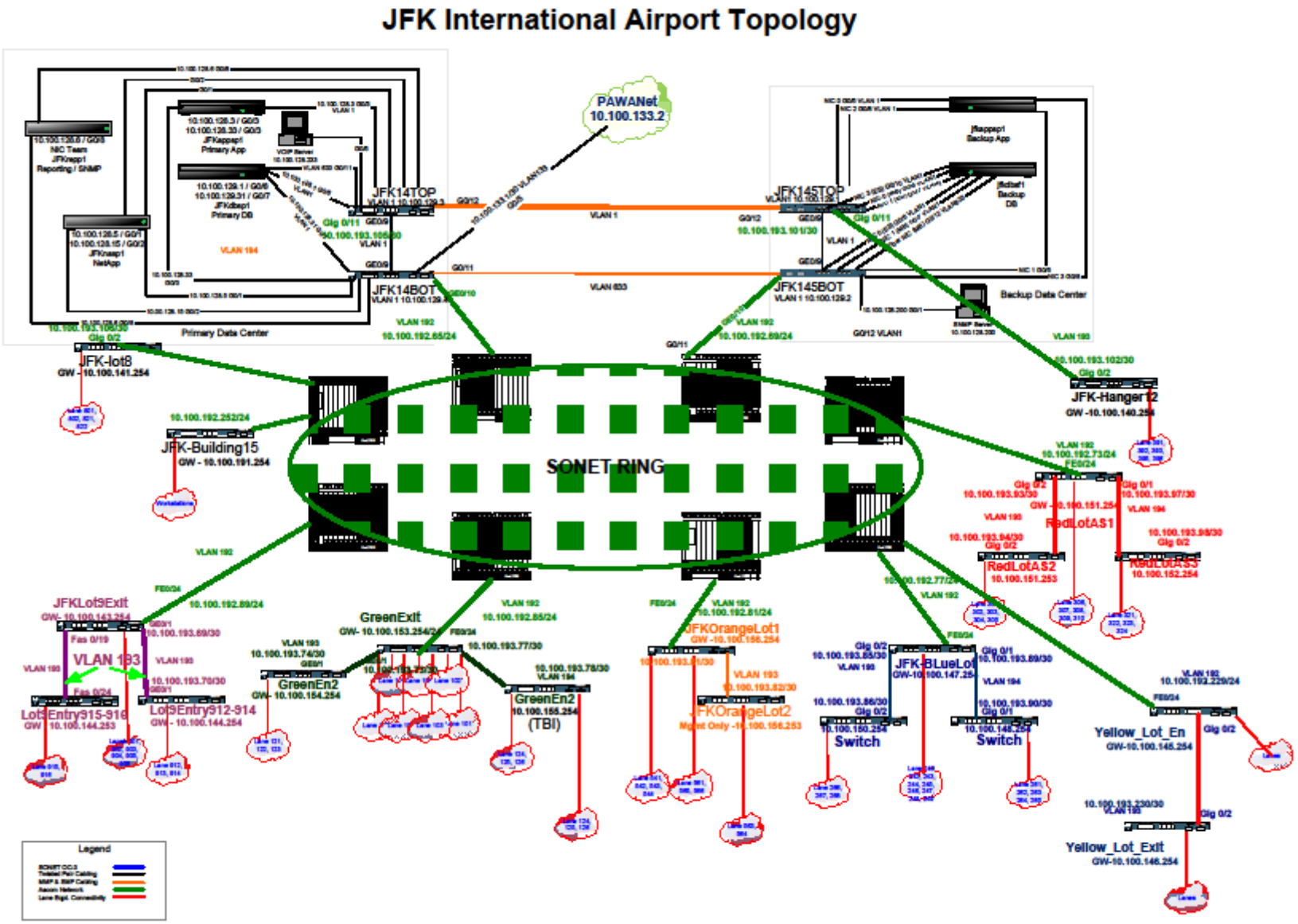
ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

EWR VLAN Infrastructure



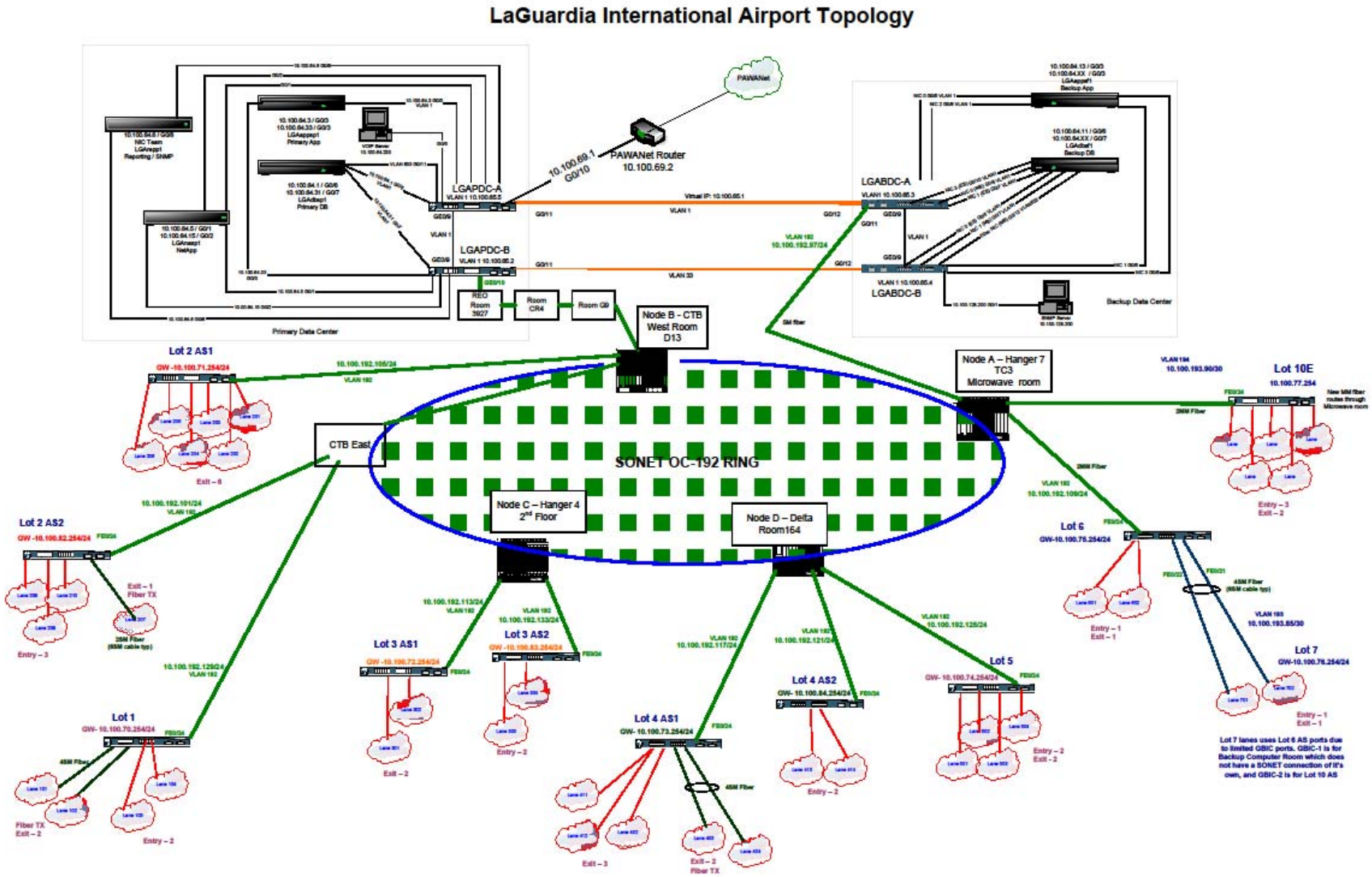
ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

JFK VLAN Infrastructure



ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

LGA VLAN Infrastructure



ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

SWF Parking Revenue Control Equipment Inventory

	Lane Number/Description	**Current Equipment**
Lot P1 - Short Term	11 / Short Term Entrance	Ticket Dispenser
		Gate
	12 / Short Term Entrance	Ticket Dispenser
		Gate
	ST exit into LT	Free Flow Gate
Lot P2 - Long Term	1 / Long Term Entrance	Ticket Dispenser
		Gate
	2 / Long Term Entrance	Ticket Dispenser
		Gate
	3 / Employee Entrance	Goose neck Stand with Card Reader
		Gate
	4 / Employee Exit	Goose neck Stand with Card Reader
		Gate
	5 / Economy to LT Exit	Ticket Reader/Validator
		Gate
	6 / Toll Booth (ADA)	Exit Booth
		ACT
		Power-Pad Unit
		Journal Printer
		Validator
		Gate
		Programmable LED Traffic Control Sign
	7 / Toll Booth	Exit Booth
		ACT
		Power-Pad Unit
		Journal Printer
		Validator

ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

	Lane Number/Description	**Current Equipment**
		Gate
		Programmable LED Traffic Control Sign
	8 / Toll Booth	Exit Booth
		ACT
		Power-Pad Unit
		Journal Printer
		Validator
		Gate
		Programmable LED Traffic Control Sign
	9 / Toll Booth	Exit Booth
		ACT
		Power-Pad Unit
		Journal Printer
		Validator
		Gate
		Programmable LED Traffic Control Sign
Rental Car Lot	10 / Rental Car Entrance	Free Flow Gate
	16 / Rental Car Exit into LT	Ticket Dispenser
		Gate
Pay On Foot Machines	13 Baggage Claim POF	Pay On Foot machine
	14 North Outside POF	Pay On Foot machine
	15 South Outside POF	Pay On Foot machine
Lot P3 - Long Term Overflow	17 / Overflow Lot Entrance	Ticket Dispenser
		Card Reader
		Gate
	18 / Overflow Lot Entrance	Ticket Dispenser

ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

	Lane Number/Description	**Current Equipment**
		Gate
	19 / Overflow Lot Exit	Exit Booth
		ACT
		Power-Pad Unit
		Journal Printer
		Validator
		Gate
		Programmable LED Traffic Control Sign
	20 / Oveflow Lot Exit	Free Standing ACT - No Exit Booth
		Card Reader
		Gate
Lot P4 - Long Term Overflow	21 / Oveflow Lot Entrance	Ticket Dispenser
		Gate
	22 / Overflow Lot Exit	Exit Booth
		ACT
		Power-Pad Unit
		Journal Printer
		Validator
		Gate
		Programmable LED Traffic Control Sign
	23 / Bus Lane	Radio Controlled gate

ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

Existing Lane Details

Newark Liberty International Airport					POF column	
Lot	**# Exit Lanes**	**# Entry Lanes**	**Bus Only Exit Lanes**	**Bus Only Entrance Lanes**	**#**	**Location**
Terminal A	0	3	0	0	3	first level
Terminal A-B	0	3	0	0	0	None
Terminal B	0	3	0	0	2	2
Terminal C Garage	0	5	0	0	4	first level
P-1 – P-3	4	2	1	0	2	2 in Airtrain stations
P-4 Garage	7	5	0	0	2	2
P-6	3	2	1	1	0	None
Employee Lot F	4	3	0	0	0	None
Mini-Plaza 1	4	0	0	0	0	None
Mini-Plaza 2	4	0	0	0	0	None
Mini-Plaza 3	4	0	0	0	0	None
Central Exit Plaza	10	0	0	0	0	None
Total	**40**	**26**	**2**	**1**	**13**	

ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

Existing Lane Details

LaGuardia Airport					POF column	
Lot	**# Exit Lanes**	**# Entry Lanes**	**# Bus Only Exit Lanes**	**# Bus Only Entrance Lanes**	**#**	**Location**
P-1	2	2	0	0	8	4 in level 1 & 4 in level 4
P-2 Garage	6	3	0	0	0	None
P-2 West Managers Lot Level 3	1	1	0	0	0	None
P-3	2	2	0	0		None
P-4	5	2	0	0	4	2 in section 429 & 2 inside terminal C
P-5	3	2	0	0	2	Walkway to the Terminal
P-6	1	1	0	0		None
P-7	1	1	0	0		None
Employee Lot 10E	2	3	0	0		None
Total	**23**	**17**	**0**	**0**	**14**	

ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

Existing Lane Details

JFK International Airport					POF column	
Lot	**# Exit Lanes**	**# Entry Lanes**	**Bus Only Exit Lanes**	**Bus Only Entrance Lanes**	**#**	**Location**
Lot 1 (Green)	7	6	0	0	2	First Level
Lot 2 (Blue)	9	8	0	0	2	First Level
Lot 3 (Red)	10	4	0	0	2	First Level
Lot 4 (Yellow)	8	3	0	0	4	First Level
Lot 5 (Orange)	4	6	0	0	2	Inside Airtrain Station
Employee Lot 8	2	2	0	0	0	None
Lot 9	5	5	1	0	0	None
Total	**45**	**34**	**1**	**0**	**12**	

ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

Existing Lane Details

Stewart Airport				
Lot	**# Exit Lanes**	**# Entry Lanes**	**Bus Only Exit Lanes**	**Bus Only Entrance Lanes**
Short Term Parking Lot P1	0	2	0	0
Long Term Parking Lot P2	0	2	0	0
Consolidated Exit	4	0	0	0
Long Term Parking Lot P3	2	2	0	0
Long Term Parking Lot P4	2	2	0	0
Rental Car Lot	1	1	0	0
Bus Lanes (to be constructed)	0	0	1	1
Total	**9**	**9**	**1**	**1**

All Airports					
Airport	**# Exit Lanes**	**# Entry Lanes**	**Bus Only Exit Lanes**	**Bus Only Entrance Lanes**	**POF**
Newark	40	26	2	1	13
LaGuardia	23	17	0	0	14
JFK	45	34	1	0	12
Stewart	9	9	1	1	
Total	**117**	**86**	**4**	**2**	**39**

ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

List of Existing Reports

Sample List of Existing Reports

- 30 day plus vehicle
- AMS Billing Detail Report
- Batch Date Payment Date Revenue Reconciliation
- Blocked Tags
- Bus_Employee Traversal Detail
- Bus_Employee Traversal Summary
- Card Number Report
- Cashier Consolidation
- Cashier Consolidation detail
- Cashier Event Log
- Cashier Exception Details
- Cashier Exit Lane Activity Register
- Cashier Exit Lane Summary
- Cashier Lane-Shift Summary
- Cashier Prepaid Activity
- Cashier Shift Summary
- Closed Service Call Response Report
- Closed Service Call Summary Report
- Company Report
- Credit Card Approved Detail Card
- Credit Card Batch Reconciliation by Payware
- Credit Card Deleted
- Credit Card Exit Lane Activity Register by Batch Close Date
- Credit Card Exit Lane Activity Register Posting Date

ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

- Credit Card Exit Lane Activity Register
- Credit Card Report Closed Batch Details
- Credit Card Report Details by Batch Date
- Credit Card Report Details by Transaction Date
- Credit Card Report Lane Summary
- Credit Card Report Lot Summary
- Credit Card Type for Facility Summary Report
- Denied Payment Type Group
- Disputes by LP
- Emergency Run Throughs
- Employee Parker Profile Report
- Entry Exit Audit
- Entry Exit Lane Activity
- Entry Lane Activity Register
- Entry Lane Monthly LPR Activity Summary
- Entry Lane Monthly Tickets
- Exit Date Payment Date Revenue Reconciliation
- Exit Lane Activity Register
- Exit Lane Activity Summary
- Exit Lane Exception Details
- Exit Lane *E-ZPass*® Activity Register
- Exit Lane *E-ZPass*® Activity Register by Revenue Date
- Exit Lane Monthly LPR Activity Report
- Exit Lane Prepaid Activity
- Exit Payment Percentage Calculation Daily

- Exit Payment Percentage Calculation Monthly
- *E-ZPass*® ACH Server Log
- *E-ZPass*® ACH Transmission History Report
- *E-ZPass*® Details by Revenue Date
- *E-ZPass*® Details Report
- *E-ZPass*® Lane Summary
- *E-ZPass*® Non Revenue Details
- *E-ZPass*® Non Revenue Details by Revenue Date
- *E-ZPass*® Reconciliation
- *E-ZPass*® Tag Event Report
- *E-ZPass*® Tag File Acquisition Report
- *E-ZPass*® Unused Tags Report
- Facility Peak Occupancy
- FAPD Daily Paid Cars & Gross Revenue Summary
- ID Report
- Login-Logout Status
- Lost Ticket Detail
- Lot Bleed Detail
- Lot Bleed Summary
- Lot Count
- Lot Duration
- Lot Exception Summary
- Lot Exit Exception Activity
- Lot Vehicle Class Payment Summary
- LPI Active Summary

ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

- LPI Exception
- LPI Images
- LPI Upload
- LPR
- Maintenance Activity Summary
- Maintenance Device and Component Parts Inventory
- Manually Entered POF Payment
- Missing Entry Transaction Report
- Missing Vehicle Report
- Monthly Lane Activity
- Monthly Stratification Report
- Occupancy Capacity Volume Analysis
- Occupancy Lane Loading
- Occupancy Transactions Flow Analysis
- Patron Vehicle Active Report
- Patron Visit Detail
- PIN & Handicap Revenue Details
- POF Activity Register
- Preventative Maintenance Report
- Problem-Resolution Summary Report
- Referred Service Call Reporting
- Returned Tags
- Service Call Register
- Special Plate Transactions
- Stock on Hand Summary

ATTACHMENT I: BACKGROUND OF EXISTING SYSTEM

- Suggested Stock Re-Order
- System Activity
- Tag Report
- Tickets Issued
- Traffic Backup Adjustments
- User Activity Performance
- Vehicle Class Payment Register
- Vehicle Inquiry Detail
- Vehicle Inquiry Detail & Summary
- Vehicle Inquiry Summary Closed Visits
- Vehicle Inquiry Summary Open Visits
- Vehicle Report
- Voided Transactions

Parking Access and Revenue Control System—Design, Installation & Maintenance

Attachment J
Audit Department Controls Requirement Contract Checklist

General

- Documented procedures, flowcharts and process maps for the application.
- Conduct regular audits, vulnerability testing, and security scanners.
- SSAE 16 SOC 2 (previously known as SAS 70 Level 2)
- Federal Risk and Authorization Management Program (FedRAMP) Certification
- ISO27001 Certification
- Criminal Justice Information Services security policies and procedures (CJIS) compliant for law enforcement information and systems.
- Background check should be performed on all personnel.

System/Security Administration

- Administrative personnel should receive training.
- Administrative staff should receive general security awareness training before access is provided. All security training must be reinforced at least every three years and must be tracked as per the PA Information Security Handbook.
- System and security administration procedures should be documented and distributed.
- Administrator(s) roles and responsibilities should be documented.
- Developers and/or programmers should not have access to the production server.
- Operating system administrators should not have access to the production database and application.

Hardening of operating system/database that supports the application:

- Disable and/or remove unnecessary ports/services.
- Remove all manufacturer samples from the production system. Scripts must be removed from production systems, except those required for the operation and maintenance of the system.
- Default, public, and guest accounts should be secured/locked/removed.
- Change all default passwords; delete all default content and login scripts.
- Limit administrative and user account privilege and access.
- Document system accounts like administrator, root, oracle, and sys.
- Document user/group access rights
    - Users/groups should be setup with least access required to perform job responsibilities.
- Implement access control at the database level (i.e. user roles and permissions, passwords, secure links)
- Use secure encrypted remote access methods.
- If the application is a web application, log (and monitor) web traffic and trend the activity looking for abnormal activity.
- Ensure that appropriate security and vulnerability assessment tools are running.
- At login, last user login should not display.
- Inventory listing of hardware and software should be current and maintained.

License Management

- Ensure that application licensing requirements are documented, reviewed and maintained.
- Application licenses should be current/valid and individuals/groups with application access should have completed the necessary access request forms and adhere to licensing requirements.

Logical Access Controls

- All users are required to read the Agency Policy Computing Resource Administrative Instruction (AI 15-4.03) and sign an acknowledgement of the Agency IT Acceptable Use Code of Conduct policy prior to account activation.
- Procedures to grant/modify/delete access should be documented.
    - Access request forms for adding/modifying/deleting users should be used.
    - Account expiration for contractors and consultants.
    - Accounts adequately identify the user – no generic accounts
- Ensure that security administrator procedures exist to:
    - Create/remove application access in a timely manner
    - Review user roles/permissions
- Validate that all users have accessed the application within the past 90 days.
    - Review dormant accounts
    - Inactive accounts should be removed.
- Each user has a unique user ID as described in the Port Authority Standard and Guidelines.
    - All user accounts profile should include Employee ID# and full user name.
- Roles are setup with least access required to perform job responsibilities.
- Roles should have a segregation of duties/roles.
- All accounts must have an individual or business group assigned to be responsible for account management.
- Segregation of duties and areas of responsibility must be implemented where appropriate.
- Whenever segregation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, audit trails and management supervision. The PA must approve these compensating controls.
- Review of audit trails and system approvals must be performed independent and retained to document the implementation of these security controls
- Access Control List (ACL) should include:
    - Current list of ACL
    - Creation and updates to ACL
    - Testing and approvals of ACL
- The application should have the PA's warning banner on the login screen. The application has a warning banner, terms of use, and/or privacy statement that was approved by the Port Authority on the login screen.
- The system should have an access role that would allow real only access to all application, database and operating system screens, functions, logs and reports.
- Remote access should be approved, secured, and documented in accordance with PA policy. Remote access, at a minimum, must consist of multifactor authentication mechanisms, secured communications (SSL/ VPN encryption methodology), access control mechanisms and logging of user activity.

a) Password Controls

- Ensure that password controls for the system are consistent with this requirements or more stringent
    - Passwords must be at least 10 alphanumeric characters long

    - Passwords must be changed every 90 days (administrators every 30 days)
    - Passwords must not be shared
    - Password complexity enable (capital letter, number, special character)
        - contain at least two upper and lowercase alphabetic characters,
        - contain at least one number (0-9)
        - contain at least one special character (e.g.-+}:>_?&$%#).
    - Accounts should be locked after a three logon failures
    - Passwords should not be the same account name
    - No concurrent login capabilities
- End user accounts will be disabled (not deleted) after 60 days of non-use.
- Password file should be securely stored with limited access and encrypted.
- Application forces initial passwords to be changed and the initial passwords should not be easily guessable.
- Maintain a password dictionary and password history should be set to 5.
- Set "automatic session timeout" to 15 minutes of inactivity and require user to log back in with valid ID and password.
- Smartphones and smart device, where capable, shall leverage biometric access to provide the most security for the least inconvenience.

Application Controls

Data Validation & Input Controls

- The application should have input controls to verify the validity of the data entered.

Data Retention and Management

- All data should be classified according to its sensitivity (confidential, etc) and protected accordingly.
- Data archive strategy should be documented and in place.
    - Should specify how long active data is kept.

Data Integrity and Security

- Sensitive data, such as credit card #s and social security #s, should be encrypted.
- Data should be restricted and audit trails should be available to identify all user activity include view access to sensitive data.
- Sensitive data should be stored in the database encrypted and blocked from user views in the application unless it is authorized.
- Encryptions level at a minimum should be AES 256bit when encryption is used.

Application Interfaces

- Interfaces should have secured transmission and be archived.
- Reconciliation of data should be done on a batch record and totals. Detail data reconciliations should be completed on periodic basis.

Processing Controls

- Application databases/interfaces should have the necessary controls to prevent processing of inaccurate, duplicate, or unauthorized transactions and producing inaccurate outputs.
- Controls to ensure that all data is processed and accounted for should be in place.
- Rejected items should be logged, tracked and resolved in a timely manner.

Change Management

- Processes and tools should be used to report, track, approve, fix, and monitor changes on the application.
- The application and all changes to the application should be tested before being put into production.
    - Documentation of approval for change and evidence of testing should be in place.
    - Specific timetable/schedule should be documented.
- Emergency procedures should be documented and distributed.
- Separate environments are required for development, test, quality assurance, production.
- Procedures should require that no changes be made directly in the production environment without going through the development/test/quality assurance environments.
- Formal change control procedures for all systems must be developed, implemented and enforced.
- Where technically feasible, development software and tools must not be maintained on production systems.
- Source code for application or software must not be stored on the production system running that application or software.
- Privileged access to production systems by development staff must be restricted.

Application Logging, Audit Trails and Record Retention

- Audit trails for operating, application, and database systems should exist and reviewed.
- Users and roles should be tracked and reviewed
    - Maintain documentation
- All failed logon attempts should be logged.
- All sensitive transactions and changes should be logged and an audit trail created.
- Audit trails should contain who made the change, when it was made, and what was changed.
- Only the security administrator should have access to change or delete these logs or audit trails.
- Audit trails should be reviewed by the business owner(s) and security administrator.
- Management reporting should be produced through the application.
- Access reports by user and privilege should be produced and reviewed periodically including access violation reports.

Contingency Planning, Disaster Recovery and Backup Management

- A business contingency plan and a disaster recovery plan for the application should be documented and stored off-site, including escalation plan and current call tree.
- Plans should be tested and the outcomes of the tests (success/failure) should be documented.
- Regular backups of the application and the application data should be stored off-site.
- Application executables should be stored off-site or in escrow.
- Application configurations should be documented and backed-up.

- Full system backup should be encrypted.
- Backup procedures should be documented.
- Tape maintenance should include:
    - Periodically testing integrity of tape
    - Procedures for tape destruction due to faulty or scratched hardware.

Performance Monitoring

- Incident monitoring procedures should be documented and incidents logs should be reviewed to ensure that appropriate action is taken.
- Performance statistics should be examined and reviewed periodically by system administrators/business owner(s).
    - If vendor(s) support the application, a service level agreement for uptime, performance monitoring, updates, etc should be confirmed.
- Baseline tools or security products should be used and checked on a quarterly basis.

Patch Management

- Patch management procedures and documentation
    - Procedures should include testing, approvals, and distribution.
    - Documentation should include emergency procedures.
- Apply all new patches and fixes to operating system and application software for security.
- All security patches must be reviewed, evaluated and appropriately applied in a timely manner. This process must be automated, where technically possible.

Physical Protection

- Physical access to the application hardware should be appropriately restricted.
    - Physical access secured by single authentication mechanism i.e. swipe card.
    - Physical security adequate for equipment (locked cabinets).
- Appropriate fire suppression systems should be in place.
- Environmental condition adequately controlled (no water, dirt, clutter) and monitored.
    - Temperature and humidity monitoring should be implemented.
- Security cameras installed in sensitive areas
- Power surge protection and emergency power backup are in place.
- All hardware and software assets must be inventoried.
- Visitors including maintenance personnel, to data center, server and network equipment storage facilities must be escorted at all times.

Anti-virus/Malware/ Integrity/Vulnerability Software Management

- Virus patch management procedures must be documented, including emergency update procedures.
- Anti-virus and software integrity checkers must be implemented to prevent and detect the introduction of malicious code or other threats.
- Virus software engines and definitions must be implemented and up-to-date.
- A remote distribution server should be implemented for virus software updates and documentation on remote distribution should be current and maintained.
- Intrusion detection system must be in place,

- All systems must have vulnerability scans performed before going into production and periodically thereafter. Appropriate action, such as patching or updating the system, must be taken to address discovered vulnerabilities.
- Host-based intrusion detection/ firewalls software must be installed and enabled on all systems to protect from threats and to restrict access. Incident response procedures must be in place to address any alerts identified and system owner should be notified of alerts and what action was taken to mitigate the issues.
- Monitoring systems must be deployed (e.g., intrusion detection/prevention systems) at strategic network locations to monitor inbound, outbound and internal network traffic.
- Monitoring systems must be configured to alert incident response personnel to indications of compromise or potential compromise.
- Procedures must be established to maintain information security during an adverse event.
- Firewalls should be implemented.
- Firewall rules documentation should be up-to-date.
- Network management connections must be performed from a secure, dedicated network.
- Network authentication is required for all devices connecting internal networks.

Wireless Device

- Devices should be using WPA/WPA2 and AES encryption or better.
- Devices should disallow broadcasting of the SSID.
- All default parameters should be changed.
- Devices should have MAC address filtering enable or some type of authentication mechanism in place.

Web Application Vulnerabilities and Controls

- The following best practice and standards from these three web sites shall be followed:
    - The Open Web Application Security Project (OWASP) - www.owasp.org
    - www.webappsec.org (a consortium of web application security professionals)
    - Center for Internet Security (CIS) – www.cisecurity.org
- Perform data validation & integrity checks for field values and ensure the HTML special characters are stripped for all HTML request.
- Do not allow site pages to be cached by user browsers.
- All sensitive, personal or confidential data (including SSN, passwords, session IDs for sensitive applications, confidential or sensitive business transactions, etc.) should be transmitted between browser and server within an SSL-encrypted session (or other encrypted transmission) and are encrypted in the database at rest.
- All sensitive and personal data should be masked and encrypted were possible.
- Legal Issues:
    - The site should have a privacy statement and term of usage.
    - American Disability Act – Section 508 should be consider during the development process due to the requirement that federal agencies' electronic and information technology is accessible to people with disabilities.
- Web Authentication: To prevent passwords from being passed in the clear, have authentication occur within an SSL encrypted tunnel. Use SSL (certificate) to protect the password.
- Password Reset:
    - For internal applications, reset passwords via the helpdesk or security administrator of the site

- For external applications, send temporary password to known e-mail address, that must be changed upon login and/or
- Have customer service reset after the user has been validated.
- If possible, use two factor authentications like Secure ID fobs.

Credit Card Processing Checklist

- If credit cards are accepted, PCI Standards (PCI DSS v3.0) should be followed and the process should be PCI compliant. Ensure all vendors and consultants are required to be PCI compliant. Attachment - The payment card application should be PCI compliant (PA-DSS v3.0).
- A segregated network and/or an approved Point of Sale terminal should be in place for the system or terminal used to process credit card transactions.
- The credit card processor standard and requirements should be followed, i.e. maintain transaction data for two years.
- Maintain the security of the customer information, including not storing credit numbers, the cardholder CVC/CVV numbers or any of the data from the magnetic strip on the credit card.
- Maintain the transaction data for contesting chargebacks, ensure that the processor fees are appropriate and do reconciliations of the transactions processed and the money deposited in the Port Authority bank accounts.
- The appropriate Port Authority functional areas should be made aware credit card processing activity and should be involved applying for the Merchant ID for MasterCard/Visa, Discover and American Express.
- Create a privacy policy and procedure for staff and consultants.
- Perform quarterly vulnerability scans of the network that contains the credit card processing, annual PCI reviews according to the PCI DSS, and annual system penetration testing.
- Perform the appropriate annual assessment and provide a report on compliance (ROC) which state shows compliance.

Disaster Recovery

The Disaster Recovery plan should include at a minimum the following areas.

- Business Impact Analysis
- Critical Time Frame
- Application System Impact Statements
- Recovery Strategy & Approach
- Recovery Time Objectives (RTO)/Recovery Point Objectives (RPO) for all critical systems.
- Disaster Definition
- Detailed Recovery Steps for each Disaster Definition
- Escalation Plans and Decision Points
- System Components- An inventory of the criticality of systems (including but not limited to software and operating systems, firewalls, switches, routers and other communication equipment).
- Disaster Recovery Emergency Procedures
- Plan Procedure Checklist
- Disaster Recovery Team Organization
  - Salvage Team & Team Responsibilities
  - Disaster Recovery Responsibilities
  - Essential Position – Require back-up personnel to be assigned.
- Contacts information Disaster Recovery Team and critical vendors - this area should be reviewed semi-annually for updates and changes.
- Post-Disaster – Detail what steps need to be taken to move from disaster mode back to normal operations.
- Contingency plans (e.g., business continuity plans, disaster recovery plans, continuity of operations plans) must be established and tested regularly.
- Backup copies of procedures, software, and system images should be taken regularly and moved offsite.
- Backups and restoration must be tested regularly.

Parking Access and Revenue Control System—Design, Installation & Maintenance

Attachment K
Technology Standards for the Port Authority

FOR RFPS

THE PORT AUTHORITY OF NY & NJ

Technology Department

TECHNOLOGY STANDARDS FOR THE PORT AUTHORITY

(Non-Confidential Sections for Use in Preparation/Distribution with RFPs)

Revised December 2015

Table of Contents

Introduction 6
1.0 The Port Authority Wide Area Network (PAWANET) 6
1.1 PAWANET Overview 6
1.2 PAWANET Circuit Diagram 6
1.3 Inter-site Services Providers 8
1.4 PAWANET Functions 8
1.5 Features of PAWANET 8
1.6 Supported Protocols 8
1.7 PAWANET Switches and Routers 8
1.8 Approved Servers 9
1.9 Enterprise Addressing Scheme (including IP addressing) 9
1.10 Enterprise Network Monitoring Software 9
2.0 Network Resources 9
2.1 Network Overview 9
2.2 Enterprise Network Architecture 10
2.2.1 Server Operating System and Software 10
2.2.2 Configuration 10
2.2.3 Network Resources Security 12
2.2.4 Network Access and User Account Security 13
2.2.5 Remote Access System 14
2.2.6 Hardware Standards 15
2.3 Network Naming Conventions 16
2.3.1 Server Names 16
2.4 Directory Services and Structure 16
2.5 System Backup and Recovery 16
2.5.1 Backup Logs 16
2.5.2 Backup Scheduling 17
2.6 Business Resumption Plan 17
2.7 Telecommunications Standards for Enterprise Network Resources 17
2.7.1 Closet and Telecommunications Room Access 17
2.7.2 Telecommunications Installation Contractor's Responsibilities 17
2.7.3 Electrical Requirements 18
2.7.4 Telephone Company Interface 18
2.8 Documentation 18

FOR RFPS

3.0 Virus Scanning & Management 19
3.1 Overview 19
3.2 Standards 19
3.3 Acquisition and Installation 19
3.4 Virus Detection and Response 19
4.0 Electronic Mail 20
4.1 E-Mail Overview 20
4.2 E-Mail System Architecture 20
4.3 E-Mail Environment: Design Considerations and Infrastructure 20
4.4 Integrating Applications Server with Port Authority Email System 21
4.4.1 Requesting SMTP Services 21
4.4.2 Email Restrictions 21
5.0 Intranet 21
5.1 Intranet Overview 21
5.2 Direction of eNet Development 22
5.3 eNet Software Infrastructure Standards 22
5.3.1 Design Standards 23
5.3.2 Accessibility Standards 23
6.0 Workstation Hardware and Operating System Software 23
6.1 Overview 23
6.2 Workstation Operating System Standard 23
6.3 Workstation Configuration 24
6.3.1 Workstation Naming Conventions 24
6.3.2 Automated Software Distribution for Computers 24
6.3.3 Remote Workstation Management 24
6.3.4 Drive Mappings 24
6.3.5 Standard Workstation Hardware Configurations 24
6.3.6 Standard Workstation Software 25
6.3.7 Enterprise Software 25
6.3.8 Other Business Applications 25
6.4 Workstation Security 26
6.4.1 Physical Security 26
6.4.2 Logical Security 26
7.0 Distributed Systems Environment 27
7.1 Overview 27
7.2 Microsoft Windows Servers 27

FOR RFPS

7.2.1 Virtual Environment 27
7.2.2 Windows Data Encryption....27
7.3 Unix....27
7.3.1 Unix Security....27
7.3.2 Backup....27
7.3.3 Download Scripts in the Unix/Linux Environment 27
7.4 z/OS....28
7.4.1 Databases....28
7.4.2 Geographic Information System....28
7.5 Application Security 28
7.6 Server Physical Security....28
7.7 Load Balancing – Failover Architecture....28
8.0 Vendor Provided Dedicated Systems....28
8.1 Overview....28
8.2 Physical Security Technology Standards 29
8.2.1 Agency Standard for Digital Video Recording, Access Control and Alarm Monitoring 29
8.2.2 Situational Awareness Platform Software 30
8.3 Communications Infrastructure Standards....30
8.4 Server Infrastructure Standard 30
9.0 Wireless Technologies 31
9.1 Wireless Standards 31
9.1.1 Purpose and Scope 31
9.1.2 General Policy 31
9.1.3 Personal Area Networks - PAN 31
9.1.4 Wireless Local Area Networks – WLANs 31
9.2 Cellular Phone & Wireless Modem....34
9.3 Technology Mobile Device Policy....34
9.3.1 Introduction....34
9.3.3 Software....35
9.3.4 Support 35
9.3.5 Training....35
9.3.6 Acquisition 35
9.3.7 Personal Acquisition 35
9.3.8 Data Security Considerations....35
9.3.9 Data Backup 35

FOR RFPS

Appendices 36
Appendix 1 -- Business Resumption Plan Document Format 36
Appendix 2 -- Communication Rooms/Closets Standards 38
Appendix 3 – Standard Cabling Schemes 39
Appendix 4 -- Unified Wiring Plan 40
Appendix 5 -- Telephone Closet / IDF Termination Blocks 42
Appendix 6 -- Workstation Jacks 43
Appendix 7 -- Standard Switches Inside the Department 44
Appendix 8 -- Workstation and Lateral Cable Identification Management 45
Appendix 9 – Fiber Optic Specification for Network Services - PAWANET 46
Appendix 10 -- Public Telephone Ordering Standards 47

FOR RFPS

Introduction

The purpose of this document is to communicate the standards established by the Technology Department (TEC) for Information Technology (IT) solutions deployed at Port Authority of New York & New Jersey (PANYNJ), the Agency.

To that end, these standards intend to help RFP Submitters do the following:

- • Implement computing and networking solutions that ensure the utmost reliability, availability and security.
- • Procure hardware and software that advances business needs in a manner that is compatible in an ever-changing IT environment that enables departments to work with each other more effectively.
- Communicate and exchange information throughout the agency easily and efficiently.
- • Achieve greater systems integration so that the application will be interoperable resulting in cost effectiveness and quality control.
- • Adherence to these standards ensures that IT investments achieve Enterprise connectivity, interoperability, consistency, and will enhance performance in a cost-effective way.

1.0 The Port Authority Wide Area Network (PAWANET)

1.1 PAWANET Overview

The Port Authority has a modern distributed computing network, called the Port Authority Wide Area Network (PAWANET), which is managed as an enterprise resource. It connects all the various Port Authority facilities and transportation systems using high-speed voice, data, and video lines or links.

This network is crucial to all Port Authority businesses because it provides the connections for applications such as e-Mail, Internet and Intranet access, SAP, PeopleSoft, Electronic Toll Collection, Computer Aided Design and Drafting (CADD), Lease Video Teleconferencing, and more.

PAWANET consist of a Managed Fiber Optic Dense Wave Division Multiplexed (DWDM) Network, provided by Verizon Select Services, as an Integrated Optical Service (IOS) network. This network consists of eleven separate and distinct (1) Gbps lightwave networks, each interconnecting with the data centers at Telecenter and the Port Authority Technical Center (PATC). Site-to-Site interconnectivity is achieved via the “hub and spoke” topology through the data centers. Additional high-speed Ethernet Private Lines (EPL) have been deployed to support key Port Authority off-ring facilities.

Remote locations are linked using redundant high-speed dedicated point-to-point leased communication lines. Wireless connectivity also supported when hardwired connections are not practical.

The network consists of state-of-the-art Cisco Systems equipment and services, such as, high performance Cisco Catalyst switches and routers. The Port Authority uses a managed Network Monitoring Services to monitor PAWANET, and Cisco Systems SMARTnet hardware/software maintenance services, and Cisco's Technical Assistance Center (TAC) to support and maintain the network. The Authority has also deployed the Riverbed network performance monitoring products to provide performance data on end user workstations and systems.

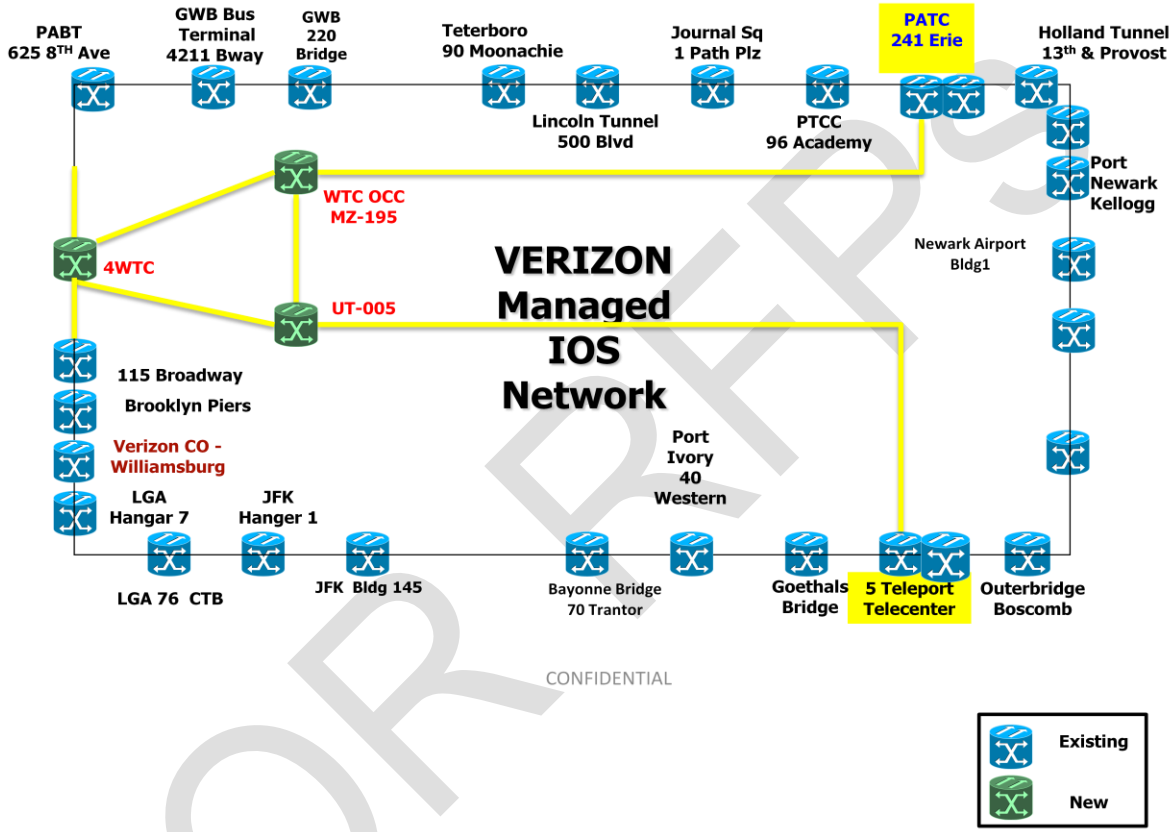
1.2 PAWANET Circuit Diagram

The current PAWANET network is being upgraded with Verizon’s Protected Riders, which will enable a seamlessly network recovery. [*Protected Riders: The Port Authority Verzion managed IOS DWDM network*

FOR RFPS

has been upgraded for additional layer of reliability. All existing Port Authority locations now support redundant dual fiber protection to avoid service outages in the event of any fiber cuts.]

The new design will replace the current PAWANET Circuit Diagram.



FOR RFPs

1.3 Inter-site Services Providers

The Technology Department (TEC) has contracted with a variety of companies to provide inter-site services Companies providing communications services for the Wide Area Network are listed below.

- AT&T Local Services
- Verizon

1.4 PAWANET Functions

Currently PAWANET is used to transport the following:

Data	Supports the low and high volume transfer of data used for applications, such as SAPand PeopleSoft, and for network communications, such as e-mail. Provides a data path for off-site, data backup of file, print and application servers. Enables the use of Storage Area Network (SAN) for network storage of user files and routing jobs to shared network printers.
Video	The transfer of Closed Circuit TV (CCTV) data is supported across the entire network to provide visibility to the Port Authority's key facilities.
Voice/VoIP	The network provides the hardware capabilities for voice and VoIP transmission. Voice over Internet Protocol (VoIP), which currently serves the majority of Port Authority users, is in the process of being implemented for the agency to replace the legacy Nortel system.
Videoconferencing	The network switches and transmission lines are used for videoconferencing to enable diversely located staff participate in meetings across large geographic area.

1.5 Features of PAWANET

PAWANET provides a high performance, resilient, and reliable fail-safe communications network. These are its key features:

- Alternate paths of communication
- Internet access
- Support of high volume traffic
- Cisco Catalyst 3000, 4000 and 6500 switches at all the major sites
- Cisco high performance 2000, 3000, ASR900 and 7200 router family products with redundant power supplies

1.6 Supported Protocols

The network supports the following network protocols, allowing dissimilar platforms to communicate within PAWANET:

TCP/IP:	TCP/IP is the universal protocol that allows communications between all systems within the Port Authority's network, as well as other networks.

1.7 PAWANET Switches and Routers

The current standard switches and routers used on PAWANET are:

- Tellabs Reconfigurable Optical Add Drop Multiplexers (ROADMS) are the Dense Wavelength

FOR RFPS

Division Multiplexing (DWDM) nodes on the Verizon Managed IOS Network.

- Cisco High performance 3000, 4000, and 6000 series switches.
- Cisco High performance 2000, 3000 series routers for intermediate connectivity.
- Cisco 7200 and ASR900 high performance routers
  Provide high-speed connectivity and routing capabilities across the network in support of TCP/IP, and provides routing capabilities for Port Authority Internet access.
- A pair of fault tolerant 10 Gbps links on IOS are installed to provide the required bandwidth between the data centers at Telecenter and PATC.

1.8 Approved Servers

Only IBM servers may be connected to PAWANET.

This includes turnkey, distributed systems, where Application servers are being used. Any replacement servers must be IBM servers. Deviation from this policy will not be allowed without prior approval of the Chief Technology Officer or their designee.

1.9 Enterprise Addressing Scheme (including IP addressing)

The Port Authority's enterprise network is a TCP/IP Class B network allowing for a maximum of 255 subnet assignments. Subnets are assigned on a geographical basis according to the number of resources required. Workstations are configured for dynamic assignment of IP addresses via Dynamic Host Configuration Protocol (DHCP).

TEC will assign static IP addresses for servers, printers, faxes and/or IP enabled device (e.g. CCTV Cameras etc.) that are to be connected to PAWANET.

1.10 Enterprise Network Monitoring Software

The Port Authority has a managed Network Monitoring Services to continually provide real time monitoring of PAWANET, and its data and voice link availability. To provide for real time network monitoring, the following software utilities are used by the Port Authority, respectively:

- Zenos Network Management software
- Cisco Works for Switched Internetworks
- Riverbed Cascade network performance monitoring software

2.0 Network Resources

2.1 Network Overview

The Port Authority has a modern distributed computing network, which is managed as an Enterprise resource. The network connects all individual PCs, servers, printers, and other devices in a unified computing infrastructure that makes it possible for the Port Authority to conduct its business.
The Enterprise Network consists of the PAWANET (see Section 1.1) and connected Local Area Networks (LAN's). The line of demarcation between the cable and wiring is the responsibility of the carrier and the Port Authority's area of responsibility is usually a wiring closet. The Port Authority's Enterprise Network consists of the following components on the Port Authority side of demarcation:

Enterprise Devices

- Cabling
- Routers
- Switches

FOR RFPS

- Wiring Closets
- Communications Equipment Racks
- Server Racks
- File and Print Servers
- Application Servers
- Storage Area Networks (SAN)
- Network Printers
- Security Devices (Video Encoders, IP Cameras, ACS Panels)

LAN Devices

- Desktop PCs
- Workstations
- Voice Over IP Phones
- Laptops
- Video Conference Units
- Local Printers
- Scanners
- Copiers
- PC Peripherals

2.2 Enterprise Network Architecture

The Port Authority operates an extensive network of Enterprise file, print and application servers. These devices are linked to an Enterprise Wide Area Network. The flexibility provided by the use of multiple servers, server clusters and Storage Area Networks (SAN) offers users improved network response, greater reliability, increased data security and reduced operating cost. Adherence to the standards outlined in this section allows the Port Authority to manage their systems, applications and data in a way that best meets our business needs while maintaining interoperability and safeguarding Port Authority's information assets.

2.2.1 Server Operating System and Software

All Enterprise servers in the Port Authority are currently based on the Windows operating system. Microsoft Windows, RedHat Linux servers, and Sun Solaris are supported as application servers when required for functionality.

In addition to the base operating system, all Enterprise servers must include or provide access to the following components:

- Virus Protection
- Network Security
- Remote Monitoring and Management
- Intrusion Detection
- Systems Backup
- Uninterrupted Power Supply (If central UPS is not installed at the location)
- Current Service Packs and security patches

Note: All standard operating system and server software will be provided and configured, by the Technology Department, prior to connection to PAWANET.

2.2.2 Configuration

All network devices--including servers, workstations, network printers, and network faxes--must use IP addresses which conform to the standards outlined in sections, 1.9 Enterprise Addressing Scheme, and 2.3.1, Server Names.

FOR RFPS

2.2.2.1 Drive Mapping Conventions and Organization

Mapping of workstation drive pointers to SAN or server disk volumes or folders is accomplished through a Windows Active Directory Login Script. The following drive letters are reserved for Windows Active Directory installations:

Pointer	Volume or Folder
M:	Reserved
P:	Public Applications
Q:	Installation and Upgrade Utilities
S:	Departmental shared directories and files
T:	Reserved
U:	Users Private Home Directory

- Public (Shared) application software installed on a file and print server cluster must reside on a separate volume named "APPS".
  Example: P:\APPS
- Each software application installed on the file and print server, or server cluster, must have its own sub-folder.
  Examples: P:\APPS\EXCEL
  P:\APPS\WORD
- Shared Data stored on a file and print server cluster, shall reside in a volume named Data, and shall be mapped to the "S:\" drive pointer.
  Example <Cluster_name>:\DATA\<Department_NAME>\SHARE on a server cluster
- Each Department's SHARE folder will contain at least three sub-folders titled Org, Everyone and Projects.
- Under the Projects folder will be two additional folders, one called "Active" and one called "Completed". Active projects reside in the "Active" folder.
- When staff identifies a project as being completed, the project folder will be moved to the "Completed" folder and all rights, except for "Browse" will be removed from the folder. This will ensure that the final project documents remain unchanged, while still allowing authorized staff to review the old documents and use them as templates for new documents if desired. The "Completed" folder will be set to archive its data.
- Under the "ORG" folder will be subfolders with names corresponding to the various divisions within the department. By default, only staff within a division will have access to a division's folder. These folders are intended to hold data for a specific division that would not normally be shared departmentally. Staff from other divisions would not have access to these folders unless the division manager of the owning division gives their approval. Having folders setup by divisions will simplify the process of identifying who is responsible for the contents of a folder.
- The "S" and "U" drives should only be used to store business related files.
- The Systems Administrator, at the direction of the Director, may from time to time remove any data deemed to be non-business related.
- A folder called "Everyone" will be created in the Share folder. All staff in the department will have full access to this folder to store and retrieve files that are not related to a project or a division's day-to-day operations.
- Additional shared folders, with access restricted to only specific users, if required, will be created in the

FOR RFPs

Share folder. Access will be restricted through the use of Windows file and folder security permissions and access will be granted through the use of groups. These groups will be named using the same name as the folder name.

- In general, rights to any folder will be granted through the use of a group having the same name as the folder. The group would have trustee rights to the folder, and users would be added to or removed from the group as needed. All rights would be granted or revoked through the use of form PA-3624A. Designated staffs in each department are required to approve these requests.
- A user "U" drive will be assigned to each standard Windows Active Directory account for use by each individual user to store business related data on the network. Access to the "U" drive is restricted to the account owner only. Users receive all rights to this folder". Users cannot share data on their "U" drive. Files should be shared only by using the Share, ("S") drive.
- Access to a user's home directory, by anyone other than the owning user is prohibited and will be removed after notifying the end-user.
- Installation files used in the installation of desktop software must reside in a sub-folder under the "APPS" volume

  Example P:\APPS\Psoft

2.2.2.2 Connecting LAN Devices to the Enterprise Network

The Technology Department (TEC) is responsible for connecting all LAN devices to the Enterprise Network (PAWANET) provided they meet the Port Authority's standards.

2.2.3 Network Resources Security

2.2.3.1 Server Physical Security

All servers and communication equipment must be located in locked rooms or secured with a cable and lock with the keyboard secured or secured with access control technology to prevent tampering and unauthorized usage.

2.2.3.2 Server Logical Security

To safeguard the Port Authority's Information Technology (IT) systems and data, TEC has implemented a number of processes and procedures, including the requirement that all users accessing the Port Authority's networks authenticate to the Microsoft (MS) Windows Active Directory (Active Directory). The Active Directory Service is a database containing descriptions of all network devices including servers, workstations and user accounts.

In plain English, this means that by executing a login when you first power on your PC you are telling the network who you are. This is accomplished by providing your Windows Username and password. Just as you are issued an ID card for access to certain facilities, buildings or rooms you need to visit to perform your job, your Windows authentication grants you access to network resources, such as shared data volumes, software applications and network printers you use in performing your assigned tasks.

TEC is responsible for providing all enterprise servers with the following protection of their logical resources:

- Guard against unauthorized access.
- Perform daily incremental backups of servers and authorized workstations and full backups weekly.
- Store all monthly backups off site at a secure location and secure daily and weekly backups on-site in a locked area.

FOR RFPS

- Test recovery procedures annually.
- Use system and application passwords that conform to the Technology Services Department standards.
- Control all remote access using the Port Authority's Remote Access System.
- Maintain current patch levels and critical security updates.

2.2.4 Network Access and User Account Security

2.2.4.1 Account Creation

User accounts are created and managed in MS Windows Active Directory Services for the Windows network resources. Documentation for the creation of user accounts and authority for access is maintained by the Customer Service Desk Manager.

2.2.4.2 Time Restrictions

Due to the fact that The Port Authority serves its clients 24 hours a day, we do not have Login Time Restrictions. All staff may access their account 24 X 7.

2.2.4.3 Concurrent Logins

Login sessions will be limited to one connection per user. User accounts should not have the ability to login to multiple workstations after establishing one active connection to the network.

2.2.4.4 Login Management

These system-monitoring features are driven by group policy and must be active:

- Restrict the count of incorrect login attempts to three before the account is locked out.
- The time for which unsuccessful login attempts are retained to determine a possible intruder attack should be a minimum of 30 minutes before the counter is reset to zero.
- The time for which a user account remains disabled before the account can be used again should be a minimum of 30 minutes.

2.2.4.5 Password Management

All user accounts must have passwords conforming to the following standards:

- a minimum of 10 characters in length
- contain at least two upper and lowercase alphabetic characters,
- contain at least one number (0-9)
- contain at least one special character (e.g.-+}:>_?&$%#).

Examples of safe passwords:

- an odd character in an otherwise familiar term, such as phnybon instead of funnybone;
- a combination of two unrelated words like cementhat
- An acronym for an easy to remember quote or phrase (see below)
- a deliberately misspelled term, e.g., Wdn-G8 (Wooden Gate) or HersL00kn@U (Here's looking at you).
- Replace a letter with another letter, symbol or combination, i.e. replacing o with zero or a "to" with 2 or i with 1.
- An easily phonetically pronounceable nonsense word, e.g., RooB-Red or good-eits .
- Two words separated by a non-alphabetic, non-numeric, or punctuation character, e.g., PC%Kat or dog,~1#

Choose a password using a phrase:

One way to do this is to pick a phrase you will remember, pick all the first or last letters from each word and then substitute some letters with numbers and symbols. You can then apply capitals to some letters

FOR RFPS

(perhaps the first and last, or second to last, etc.)

Examples **Phrase**	**First Letters**	**Password**
"Double, double, toil and trouble; Fire burn, and cauldron bubble!"	ddtatfbacb	Ddt@t:fb@cb
"Every time I try to get out, they pull me back in."	etittgotpmbi	3t1ttgoTpmb1
"You Can't Have Everything. Where Would You Put It?"	ychewwypi	Uch3Wwup1?

- Smartphones, where capable, shall leverage biometric access to provide the most security for the least inconvenience.
- User passwords will require a change every 90 days.
- All accounts will be granted the minimum level of access and permissions necessary to perform an assignment.
- If a system account fails to satisfy the requirements of this policy, an administrator may place the account in "disabled" status until remedied.
- Changes to an account's access privileges require the appropriate managers to request new or modified access.
- All users are required to read the Agency Computing Resource Administrative Instruction and sign an acknowledgement of the Agency IT Acceptable Use Code of Conduct policy prior to account activation.
- Annually, all managers are required to certify that only authorized employees have accounts on Agency systems. Technology and the Office of the CSO will work with managers to provide them with the lists of employees and their accounts.

Passwords are considered confidential data. They protect the Port Authority's network resources and grant system privileges and access. Disclosure may result in unauthorized access to data, system files and transactions. Passwords are also your signature and identify you as the individual who is responsible for the system activity.

2.2.4.6 Modems and Switches

Staff is prohibited from connecting dial-up modems and switches including wireless switches (e.g. Linksys wireless switches) to workstations that are simultaneously connected to PAWANET or another internal communication network unless approved by the Technology Department (TEC).

Where modems have been approved, users must not leave modems and/or switches connected to personal computers in auto answer mode, such that they are able to receive in-coming dial-up calls.

2.2.5 Remote Access System

The use of local modems to establish direct dial connections to devices on the Port Authority's network is prohibited. Exceptions to this policy require the approval of the Technology Department's Chief Technology Officer.

The approved mechanism for remote access to the Port Authority network is through the Remote Access System (RAS). The Remote Access System utilizes an Internet-based Virtual Private Network (VPN) tunnel established over the Internet linking remote users to the Port Authority Wide Area Network (PAWANET) (remote client to PA site). It is designed to provide authorized Port Authority users with secure access to corporate applications and to files available on their departmental file servers. Once connected to the PAWANET, users with PA-supplied laptops will have access to computing resources as if connected directly to the network. For users using non-PA remote desktops/laptops, once connected to the network, access to applications and resources is delivered through a thin-client environment consisting of a farm of Citrix XenApp/Microsoft Terminal Services servers capable of supporting 200 or more simultaneous users each.

FOR RFPS

There is no provided access to the user's office PC desktop. Port Authority offices without direct connection to the Port Authority Wide Area Network (PAWANET) can use this system to establish remote access to corporate applications located on PAWANET.

RAS provides multiple security mechanisms to ensure that only authorized users gain access to the Port Authority's computing resources and systems. Through multiple security steps, the user must respond to security challenges. After successful authentication verification, authorized users are provided with access to corporate applications and their departmental network resources.

The Port Authority also supports corporate site-to-site VPN connections and utilizes Cisco equipment for these connections.

Remote access is authorized on a case-by-case basis by the Chief Technology Officer.

2.2.6 Hardware Standards

The TEC Enterprise Architecture team is responsible for setting the Agency hardware standards. As of August 2015, the hardware standards are as follows:

Desktop, Laptop, CAD*	Lenovo, Microsoft, Panasonic Tough Books
High End Multimedia Workstation*	Apple
Printers	HP, Lanier
Routers and Switches	Cisco
Servers*	IBM
Smart Devices	iPhone/iPad
Storage Area Network (SAN)	IBM (Entry Level and Mid-Range)

*Note: To maintain optimal operating efficiency of the computing environment a standard "Refresh" age has been adopted. The Agency standard refresh age is greater than or equal to 5 years. TEC is responsible for the automatic replacement/upgrade of hardware that has exceeded the Agency standard age limit.

2.2.6.1 Standard Servers

A representative sample of standard servers is as follows (As of August 2015):

Server Description	**IBM Model**
WEB Server, Small applications server	xSeries 3550M4
Medium applications server	xSeries 3650M4
Database Server, Multiple and Large application server	xSeries 3850X5
VMWare Clusters	NEC Express 5800 series or IBM as stated above

Each server shall have at least two (2) network interface ports to support a production, management and backup network, and redundant power supplies.

The Port Authority manages servers models via a lifecycle process with a minimum 'in service' life of five (5) years.

FOR RFPS

2.3 Network Naming Conventions

2.3.1 Server Names

The Port Authority employs a naming convention for all servers within PAWANET. That convention will be discussed during a solution implementation phase.

2.4 Directory Services and Structure

The Port Authority uses Windows Active directory to manage network resources and user access. Port Authority departments are designated as organizational units (OU) and servers are network objects contained within the OU.

All network printers should be created using Printer Properties Pro utility.

Applications are distributed using Microsoft System Center Configuration Manager (SCCM).

Applications are distributed based on the type of workstation and user definitions.

Scheduling of distributions is performed in conjunction with client departments.

2.5 System Backup and Recovery

There are two Port Authority approved standard software products, used to perform scheduled server backups:

- **Upstream Reservoir** is a centralized backup tool used to create data backups for all distributed systems.
- **FDR Upstream** is a Mainframe based tool used to backup all Mainframe data.

Backup data is stored on disk storage for prompt backup and restore. Encrypted tape backup is stored remotely at a secure facility, and is required to assure off-site disaster recovery data storage. All backup media and records must be treated with the same level of security and confidentiality as the original data.

The System Administrator is responsible for verifying that system backups, both local and remote backups, can be used to restore the data. Tests of the ability to successfully restore from both backup systems should be performed annually. It is recommended that:

- Tests of the ability to restore system and application files will be performed on a non-production server.
- When incremental or differential backups are routinely used, the test restore procedure should incorporate both.
- Immediately prior to performing the test restore procedure, do a special full backup on the directories being tested.

2.5.1 Backup Logs

The System Administrator will maintain the following logs for a period of two years:

- Back-up activity
- Rotation of back-ups
- Usage/rotation of back-up media
- Off-site data storage

FOR RFPS

2.5.2 Backup Scheduling

The System Administrator is responsible for performing back-ups of data, application and system files. This must be as follows:

- Weekly full back up of each server. A full back-up is a back up of all files on the server.
- Daily differential, incremental or full back up of each server or server cluster. The type of back-up performed is dependent on time constraints and the amount of data to be backed up. Incremental back ups are back-ups of all files changed since the last back up. Differential back ups are back-ups of all files changed since the last full back-up.
- A Grandfather, Father, Son (GFS) scheme based on a 33 tape rotation should be used to ensure complete back-up and recovery.

2.6 Business Resumption Plan

The vendors, providing IT services to the PA, shall work with the Technology Department (TEC) to develop a disaster recovery and contingency plan. The System Administrator will participate in the planning, design, implementation, testing, updating and documentation of the plan. Appendix 1 shows a recommended outline for such a plan. The Business Resumption Plan shall be updated and tested at least annually.

2.7 Telecommunications Standards for Enterprise Network Resources

To see the standards for the following telecommunications components, please see the Appendix.

Appendix 2 - Communication Rooms/Closets Standards

Appendix 3 - Standard Cabling Schemes

Appendix 4 - Unified Wiring Specifications

Appendix 5 - Telephone Closet / IDF Termination Blocks

Appendix 6 - Workstation Jacks

Appendix 7 - Standard Switches

Appendix 8 - Workstation and Lateral Cable Identification Management

Appendix 9 - Fiber Optics Specifications for Network Services - PAWANET

2.7.1 Closet and Telecommunications Room Access

The following standards must be followed regarding access to closets and communication rooms:

- All telecommunications rooms must be physically secured. Remote locations, which are not secured, by a guard or within line of sight of personnel, must be secured by a card access system and/or video cameras.
- The Network Connections (NC) group is responsible for installing routers, switches (along with Cisco Staff when applied) and station drops. They also patch connections and troubleshoot LAN cabling.
- System Administrators requiring routine maintenance of data communications equipment should call the Customer Support Desk when new devices or reconfigurations are required.

2.7.2 Telecommunications Installation Contractor's Responsibilities

1. Adherence to all of the above specifications
2. Assurance of labor harmony
3. The contractor must supply all cable, blocks, brackets, connectors, jacks, housings, face

FOR RFPS

plates, special tools, etc., as necessary to perform an installation which is satisfactory to the Port Authority.

4. The contractor must label every workstation (jack faceplate) and the corresponding cross connect point (punch down block or patch panel) in accordance with the cable identification management plan, as previously described.
5. Install all Category 5e/6 cabling in the proper manner, with the appropriate number of twists, to maintain Category 5e/6 integrity and capabilities, as outlined in the TIA/EIA 568-B.2 standard.
6. The contractor must ensure that cable connections are in accordance with standard telecommunications practices and that all cabling maintains normal connectivity and continuity.
7. All materials must be agreed upon by PA Network Services prior to the start of installation.
8. All computer or network communication rooms and closets are to be isolated, locked, and secured. No other equipment, storage area, or smoking area are to be located in this room. This room must provide appropriate cooling and ventilation. Access to this room will be reserved to TEC staff and an agreed upon Facility Manager or designee of the site where the PAWANET equipment is located. This procedure is to ensure the security and the integrity of the Port Authority's computer network and its users.

2.7.3 Electrical Requirements

The following power and receptacles should be installed to support different equipment requirements such as:

- Standard 110/120 volt power receptacles
- Standard and/or NEMA L6-30P 220/240 volt 30 amp power receptacles
- Dedicated circuit breaker per AC feed, with alternate power source.
- Server rack electrical requirements are specified in the appropriate design document.

Currently, services obtained through the PA's contract are required to have the APC (American Power Conversion) UPS included in the delivered service.

2.7.4 Telephone Company Interface

The following items are needed for the telephone company interface, if needed for a specific vendor solution:

a) Install a dedicated wallboard for Telco demarcs (if none available for implementation)

b) Standard Telco demarcs:

- P66 Block
- Network Termination Unit (Rj48 interface) Smartjacks
- Network Termination Unit (DB15-pin female interface)
- Network Termination Unit (V.35/V.36 female interface)
- Digital Signal X-connect (DSX)
- Basic T1 CSU/DSU
- Basic DS3 handoff coax/HSSI unit
- High-speed dialup modems for network trouble-shooting when needed

2.8 Documentation

It is the responsibility of the System Administrator to update and maintain a library of all documentation designated as standard by the Port Authority. These include archived system files and system backups. Vendors will be provided our "Guide to Systems Administration" during the implementation phase of a project. The "Guide to Systems Administration" covers the provisioning and setup of computing &

FOR RFPs

networking resources to successfully implement a project within the Port Authority. Vendors will work with TEC during implementation to ensure proper setup, configuration and connectivity to PAWANET.

3.0 Virus Scanning & Management

3.1 Overview

This section describes the standards for the prevention, detection and removal of computer viruses, (malware). Its purpose is to minimize the risk and negative impact of computer virus infections in the work environment by establishing clearly defined roles, responsibilities and procedures for the effective management of computer viruses.

3.2 Standards

Standard virus protection software must be installed on all network servers and personal computers, and updated on a regular basis. The Port Authority currently uses McAfee ePolicy Orchestrator (ePO) to monitor, manage and maintain the virus definition (DAT files) of the Agency desktop computing platform. The McAfee ePO Management Agent, and VirusScan / AntiSpyware Enterprise, are part of the standard desktop core image.

3.3 Acquisition and Installation

The Technology Department maintains current versions of standard virus protection software and virus detection files, (DATs), including configuration-specific instructions for downloading and installing the software on network servers and desktops.

3.4 Virus Detection and Response

The Technology Department is responsible for responding to all virus outbreaks, as well as eradicating them and, where possible, preventing them.

The speedy reporting of all computer viruses is essential for the protection of the information stored on Port Authority LANs. Much of that information is important to the safety of the public, as well as the day–to-day business of the PA.

If the anti-virus software has detected a virus and cleaned it, no further action is required on the end user's part. If the virus is not cleaned, or the end-user suspects that a virus still exists, the end-user should immediately contact the Customer Support Desk, and they will work to remove the virus. The Technology Department will respond quickly to all such alerts by doing the following:

Assess the risk

- Confirm the existence of a virus.
- Take appropriate measures to quarantine the virus so that it does not infect other Port Authority devices.

Notify Appropriate Parties

- Contact the originating party who introduced the virus to the Port Authority.
- If it is a new virus, contact our antivirus vendor, McAfee, for further assistance.

Remove the virus

- Work with appropriate parties until the virus is removed.

In addition, the Technology Department will report on all such outbreaks on a weekly basis. The report must include:

Support Ticket Number
User Name
Virus Name
Information which was lost, (if any)

FOR RFPs

Time to correct the problem, (lost staff time)
Virus Origin, (if this can be determined; Diskette, CD, Internet)

4.0 Electronic Mail

4.1 E-Mail Overview

The Port Authority's Electronic Mail System (E-Mail) is designed to facilitate business communication among employees, job shoppers, contractors, consultants, and outside business associates. This E-Mail system is comprised of Microsoft Outlook desktop software accessing e-mail stored on Microsoft's Office 365 Exchange Online servers. This solution also includes group calendaring and workgroup collaboration.

4.2 E-Mail System Architecture

The Port Authority's E-Mail system is hosted by Microsoft as part of its Office 365 government cloud services offering. Authorized Port Authority staff access their corporate e-mail through Microsoft Outlook desktop software as well as via Outlook Web App and through mobile devices. The Office 365 Exchange Online system has multiple Exchange servers containing mailboxes and Public Folders, and performs Internet-based e-mail services including anti-spam and anti-virus e-mail checking. More in-depth knowledge about the Microsoft Office 365 government cloud can be found on the Microsoft website.

Office 365 is accessed using the Port Authority's corporate user account which is hosted on the Port Authority's active directory platform. In addition, the Port Authority hosts DNS servers to satisfy requests from the Outlook client as needed.

High-speed, secure, and redundant network connections provide access to the Internet including to the Office 365 cloud from the Port Authority network.

4.3 E-Mail Environment: Design Considerations and Infrastructure

The Office 365 e-mail environment is further described below:

- The e-mail system is comprised of Microsoft Outlook 2007 desktop software accessing e-mail stored in Microsoft's Office 365 government cloud service. A current project will update the desktop environment to Office 365 Pro-Plus (Office 2013) and is tentatively expected to be completed by 12/31/2015.
- E-mail is protected by Microsoft's Exchange Online Protection.
- There are several forms of SMTP addresses used at the Authority.
- Exchange Active Sync and a cloud-based MaaS360 Mobile Server is used to provide e-mail and calendar access and control to Apple iPads/iPhones and Windows Mobile devices.
- Exceptions are governed by the Authority's directory services structure and user account requirements.
- Each individual e-mail message and its file attachments, the overall mailbox size limitations, and additional features are governed by the current Microsoft Office 365 government cloud specifications which can be found on Microsoft's web sites.
- This e-mail system also includes group calendaring and workgroup collaboration.
- Public Folders are supported based on departmental and agency-wide requirements and, in general, are used for dynamic items for a form of workgroup collaboration. Email-enabled public

FOR RFPS

folders have been phased out and replaced by Office 365 Shared Mailboxes. Static documents like corporate policy statements are placed on the corporate intranet (EmployeeNet) and not on the Public Folders. Documents requiring long-term storage are stored elsewhere such as on Windows file servers.

4.4 Integrating Applications Server with Port Authority Email System

4.4.1 Requesting SMTP Services

The vendor will request SMTP services from and coordinate its work with the Technology Department.

Port 25 needs to be available to utilize it for SMTP services.

4.4.2 Email Restrictions

The following restrictions are in place to protect the SMTP system and the "reputation" of Agency mail servers on the Internet:

- Forged email headers are STRONGLY discouraged, but applications for circumvention will be entertained, and valid business justifications must be included. The "From" and "Reply-to" fields should be valid users on the system sending email.
- Settings: The maximum number of recipients per email is currently 90. This includes "To", "cc", and "bcc"; maximum size with attachments is defined by O365 Limitations. Emails that do not conform to these restrictions will be rejected by the SMTP servers.
- Mail will be relayed only if your server has an entry in the SMTP access database.

Note: SMTP logs are checked periodically for policy violations. Repeated violations and failure to correct them will result in SMTP services being disabled for the offending system.

5.0 Intranet

5.1 Intranet Overview

The Port Authority EmployeeNet (eNet) is intended to provide timely information and resources to employees via the web browser on their desktops. eNet is a decentralized collection of web pages, data lookup services and applications that are managed as if they were a centralized enterprise resource. It is accessible to all personal computer workstations on the Port Authority Wide-Area Network (PAWANET). eNet is housed on servers at the Teleport and PATC Data Centers.
Examples of business information hosted on eNet include:

Departmental Websites
Directories
Corporate Announcements
Reference Materials
Document Collections
Library Services
News Displays
Enterprise and Departmental Applications

FOR RFPS

5.2 Direction of eNet Development

eNet is intended to provide a convenient, timely and accurate source of information for Port Authority employees as well as providing access to enterprise and departmental applications. The owner of content on eNet is responsible for authorizing its publication, its accuracy and timeliness. Technology Services provides a common infrastructure and technical support for those departments that electronically publish agency information or make available electronic resources. Infrastructure standards are recommended to ensure compatibility and facilitate maintenance. Departments requesting specific applications should discuss their requirements with eNet staff to determine a solution that best meets the department's business needs.

5.3 eNet Software Infrastructure Standards

Category	**Software Name**
Browser:	Microsoft Internet Explorer
Browser Plug-in:	Windows Media Player
	Adobe Acrobat Reader
	Macromedia Shockwave Player
Web Server Software:	Sun One Web Server
	Microsoft IIS
Media Server Software	Microsoft Media Server
Application Server Software:	Adobe Cold Fusion 10
Development and Design Tools:	Adobe CS5
Database	Oracle Database
	MS SQL Server
	MS Access
Programming Language/Scripts	ColdFusion MX 10 JavaScript
Search Engine	UltraSeek (software) Google Mini Search Appliance (hardware)

FOR RFPS

Category	Software Name
	MaxxCAT Search Appliance (hardware)
Web Performance Monitoring:	Google Analytics WebTrends Marketing Lab 2
Content Management:	Open Text Website Management

5.3.1 Design Standards

We have developed the following standards to ensure that all web pages on eNet have a consistent look, feel and navigation scheme, while providing creative flexibility.

Departmental Web Site Standards

Prescribed standards are assigned to only the following items:

Resolution:	Pages are designed for optimal viewing at the 1024x768 setting.
Page Width:	Each page has a fixed page width of 960 pixels.
Page Justification:	The entire page is center-justified within the browser window.
Page Layout:	Each web page will follow the same, basic layout: A Global Navigation strip; A Masthead; A Local Navigation strip; A Body area (with a 1-column, 2-column or 3-column layout); A Footer.

5.3.2 Accessibility Standards

TEC's eBusiness Unit is committed to making all eNet content accessible to persons with disabilities. In order to ensure that all eNet web content is in compliance with accessibility standards and applicable legal requirements, contact the Webmaster via email at webmaster@panynj.gov, or call 212-435-3294.

6.0 Workstation Hardware and Operating System Software

6.1 Overview

The Port Authority makes extensive use of computers (workstations) networked into an Enterprise Wide Area Network to accomplish its business objectives. For the purpose of this section, the term computer and/or workstation will be used to reference desktop, laptop and CAD computing devices. In order to ensure compatibility with the agency's enterprise network and to make optimal use of its resources, this section defines the standards governing workstations and their configuration and use.

6.2 Workstation Operating System Standard

The Port Authority's standard operating system for workstations is Microsoft's Windows 7. The following are operating systems used within the Agency:

- Microsoft Windows 7, Enterprise
- Apple OS X

FOR RFPS

6.3 Workstation Configuration

6.3.1 Workstation Naming Conventions

All departmental workstations must contain a unique computer name which is the machine's serial number.

Example: Workstation name: 23AAH86

System Administrators are responsible for naming workstations and maintaining an up- to-date inventory of equipment and names used.

6.3.2 Automated Software Distribution for Computers

The Port Authority currently uses Microsoft System Center Configuration Manager (SCCM) 2012 to, at a minimum, do the following:

- Install new, or upgrade existing, software on Agency desktop, laptop, and CAD computers.
- Create packages to automate system tasks (e.g. data migrations of desktop computers, eDiscovery requests, etc.).
- Bare Metal Provisioning of Servers.

6.3.3 Remote Workstation Management

The Port Authority also distributes software applications and upgrades via Microsoft's SCCM. Each workstation should have Microsoft System Center 2012 R2 Remote Control Viewer installed as part of the workstation client. This will enable remote distribution and updates of software, hardware inventory and workstation troubleshooting. Microsoft security patches are distributed through a PatchLink agent.

6.3.4 Drive Mappings

Computer drive mappings are automatically accomplished using a Microsoft login script. The script is executed upon successful login to the Agency's Microsoft domain.

6.3.5 Standard Workstation Hardware Configurations

The Technology Department is responsible for setting the computer hardware standards. Standards are typically set annually, or as exceptions to meet business requirements. The standards specify the approved hardware components required by the Agency for a specific computing platform (e.g. desktop, laptop, CAD). The following is current workstation standard:

Lenovo ThinkCentre M93p Tower 10A6S19900-PA (PC)
Lenovo ThinkStation P500 30A6S0MM00 (CAD)
Lenovo ThinkPad T440 20AWS2EV00-PA (LAPTOP)
Microsoft Surface pro
MONITORS
NEC AccuSync AS203WMI-BK (20 Inch Wide Flat Panel)

FOR RFPS

NEC MultiSync EA244WM1-BK (24 inch Wide Flat Panel)
[redacted]

6.3.6 Standard Workstation Software

The following software is the standard Port Authority software for departmental workstations. New computer installations should conform to the existing standard.

6.3.6.1 Standard Workstation Software

The following list is a compilation of the core software components found on each computer (commonly referred to as an image).

Windows 7, Windows 8.1
McAfee Antivirus
Internet Explorer
Microsoft Office Professional
Printer Pro
Java
Lumension End-Point Protection
Remote Access Software (for laptops)

Because technology is rapidly changing, TEC should be consulted to obtain the most recent versions of standard software.

6.3.7 Enterprise Software

The following is a list of standard enterprise application software used in the Agency. These applications are supported by third-party service providers:

PeopleSoft
SAP
Enterprise Connect (Livelink) Content Management
One Drive for Business
SharePoint/Online
Skype for Business

6.3.8 Other Business Applications

Other Enterprise applications are deployed on occasion to user workstations. This includes systems like BudgetPro. System Administrators are responsible for deploying the workstation clients and network server software according to standards provided by Technology Department:

Current list of Enterprise applications, is shown below –

- AutoCAD
- BudgetPRO
- Cognos Client Software
- EBS (Emergency Broadcast System)
- Enterprise Connect (Livelink)
- HIDS,
- Lumension (PatchLink),
- McAfee Virus Scan and AntiSpyware Enterprise
- MS SQL

FOR RFPS

- Oracle
- PeopleSoft
- Primavera
- SAP
- Schedulesoft
- TRIM

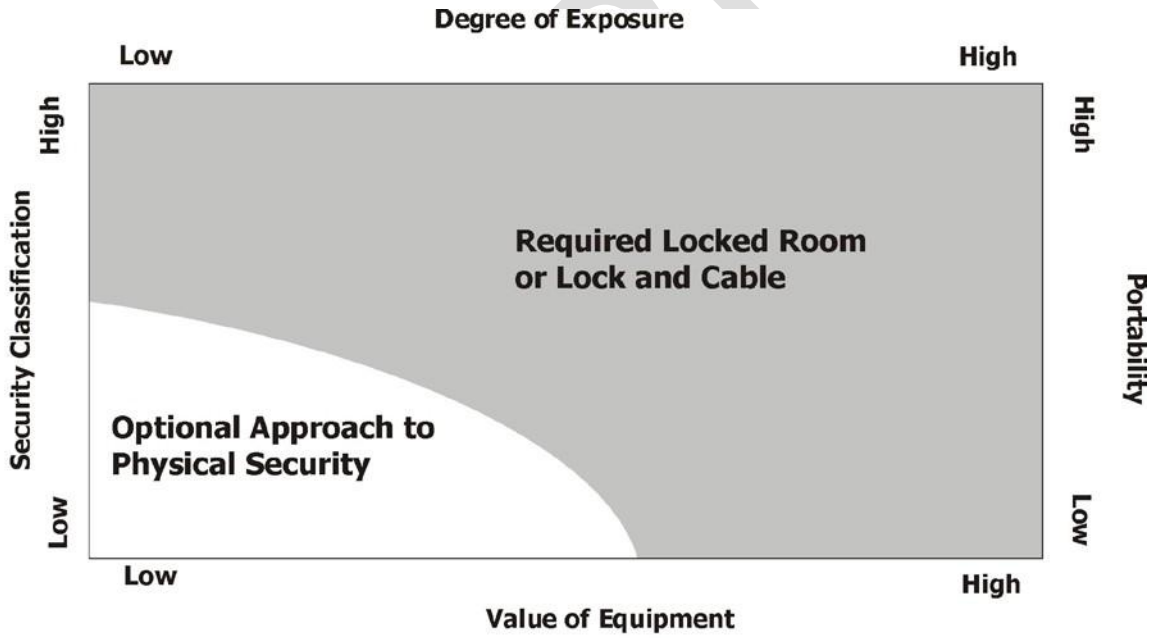
6.4 Workstation Security

Workstation users and their managers are responsible for the security of computer equipment and safeguarding critical corporate data and access to Port Authority network resources. This includes both the physical securing of equipment as well as logical safeguarding equipment and data.

6.4.1 Physical Security

The method of control should be based on the value of the equipment, the sensitivity of the data, its portability and the degree of exposure to theft. The department's Business Manager should make the appropriate determination of physical security required based on their best business judgment.

The graph below provides general guidance to Business Managers in determining the level of physical security required.



In all cases, laptops must be secured with a Lock/Cable product (e.g., Kensington).

6.4.2 Logical Security

The Technology Department (TEC) is responsible for providing for the security of computer resources and devices:

- Workstations are protected with Microsoft directory security mechanisms.
- Screen saver passwords are implemented with a maximum of a fifteen (15) minute time-out.
- All critical data on a network drive are backed up nightly onto either external media or a network storage.

7.0 Distributed Systems Environment

7.1 Overview

A number of enterprise servers provide critical application and system services. Different operating systems and configurations may be required for specific applications. This section provides information on the standards for supported systems within the Port Authority.

7.2 Microsoft Windows Servers

The standard for general-purpose application servers and File and Print Computing is IBM servers. Microsoft Windows 2008 Server (Enterprise) and 2012 Server are currently supported Operating Systems for application servers.

7.2.1 Virtual Environment

The standard for Virtualization Computing is IBM host servers. The Port Authority will provide a VMware ESXi-based Guest Virtual Machine (VM) to operate all Contractor-provided applications software.

All applications software will be capable of operating in a virtual environment under VMware ESXi server and will operate in a VMware ESXi-based Guest Virtual Machine (VM) on a 'shared' host-computing platform for Contractor application, unless performance or other requirements mandate a dedicated system.

7.2.2 Windows Data Encryption

For those applications that require additional data security measures, TEC offers additional tools that provide encryption services to protect the data stored in the application's database or file and folders, even from authorized individuals that have physical access to the applications and database servers but not the decryption key.

7.3 Unix

Sun/Oracle Solaris and RedHat enterprise Linux are the currently supported UNIX operating system for infrastructure and corporate servers.

7.3.1 Unix Security

Unix and Linux servers must be physically and logically secured from unauthorized access. Operating system logical security is defined by the Technology Department (TEC).

7.3.2 Backup

Critical system backup must be performed regularly (daily and/or weekly) utilizing our centralized backup strategy and associated tools. Extra copy of backup is kept offsite for disaster recovery purposes if required.

7.3.3 Download Scripts in the Unix/Linux Environment

- The script must be written in a generally supported language: Perl, Korn shell, PowerShell. PowerShell will be consistent with Microsoft standards and best practices.
- The script must be limited in access, as well as the script's owner's user account. The owner of the script should be able to read, edit, and execute the script, but no one else (with the exception of the root or administrator accounts).
- If the content being downloaded is public information or widely available on the Internet, File Transfer Protocol (FTP) may be used.

FOR RFPS

- For all other content, Secure FTP must be used, and a key exchange made with the entity who is providing the content. A username and password must be used when retrieving the content.
- If the entity cannot accommodate the use of SFTP, ftp may be used as long as the content is encrypted with a secure, widely used utility like PGP.
- Information and guidance on securing passwords should follow Recommendations of the National Institute of Standards and Technology.

7.4 z/OS

z/OS (currently release 1.5) is the IBM-supplied operating system on the IBM 2096-R07. This hardware/software supports multiple users and multiple applications. Provided on this platform for transaction-processing applications are TSO/E, ISPF, and CICS. The database is DB2, although other file structures are also supported. The Agency is dis-investing from this operating system and it will not be used to support additional applications.

7.4.1 Databases

Oracle 11gR2 or higher and MS/SQL Server 2008/2012 or higher are the supported database platforms for Port Authority systems. Auditing trail enabled for all database accounts with administrator privileges.

7.4.2 Geographic Information System

The Geographic Information Systems (GIS) is built on an ESRI platform using ArcGIS for Desktop version 10.2 and ArcGIS for Server version 10.2. GIS data are stored in geodatabases using SQL Server 2012.

7.5 Application Security

TEC recognizes the critical importance of application security and maintains a Best Practices document containing rules and recommendations for purchased applications, and those developed in-house.

7.6 Server Physical Security

All servers and communication equipment must be located in locked rooms or secured with a cable and lock with the keyboard secured to prevent tampering and unauthorized usage. The Business System Manager is responsible for determining the appropriate access control method (receptionist, metal key lock, magnetic card door locks, etc.) This person must also maintain a list of persons authorized to enter secured areas. Technology Department staff is available to provide technical assistance in making this determination.

7.7 Load Balancing – Failover Architecture

Depending on the requirements of the application, load balancing and failover architectures are supported.

8.0 Vendor Provided Dedicated Systems

8.1 Overview

Vendor Provided Dedicated Systems refers to the application software and possibly the computer hardware that may be furnished and/or installed by an outside contractor. These systems are usually procured through either a Request for Proposal (RFP), or a “Low Bid” contract and are specifically engineered to support a dedicated application.

FOR RFPS

These systems generally support Capital Projects, which are usually large scale, multi-year engagements, requiring specialized technical and management staff, as well as, Systems Integration support. These projects normally have significant construction components and require the coordination, design and support from many diverse Engineering and Technology disciplines.

On all technology related projects a representative from the Technology Department (TEC) provides a single point of contact for technology oversight, accountability, adhering to standards and systems integration, which is required under the Roles and Responsibilities of the Director and is expected by our client departments.

To ensure a successful project implementation and honoring our responsibility to the Agency and our customers, one of the steps undertaken by TEC is to provide guidance and focus attention on, adherence to and compliance with the Port Authority Technology Standards.

By following the Technology Standards, it enables the Port Authority to

- Leverage large discounts negotiated in the various requirements contracts.
- Ensure that the seamless integration of equipment with other existing systems.
- Ensure that long-term maintenance and systems administration contracts are focused on the same product lines.
- Ensure that the relevant sections of the Technology Standards are included in either, the basic design of a low bid contract or as requirements in an RFP. Responses to RFP's shall be reviewed for their compliance with the Technology Standards.
- Deployment, integration and testing shall be monitored by TEC to ensure that equipment or infrastructure is not duplicated, that the integration and migration plan will not adversely affect existing systems, and to integrate new systems under existing maintenance contracts where applicable.

In cases where a specific vendor or system is so specialized that it normally does not adhere to the hardware, software, infrastructure and operations standards of the Technology Standards, the vendor shall be directed to work with TEC in exploring all options. If an exception is required, the vendor should work with TEC to prepare the necessary business case scenarios to receive written concurrence from the CTO for this deviation from the Port Authority Technology Standards.

8.2 Physical Security Technology Standards

8.2.1 Agency Standard for Digital Video Recording, Access Control and Alarm Monitoring

Based upon the Agency's investment and positive experience with commercial leaders in access control and alarm monitoring application, CCTV and Digital Video recording technologies. The Agency has developed a standard for these business functions.

The Port Authority has long recognized the need for a corporate architecture for its security systems that would allow us to integrate digital video and access control recording compatible technologies agency-wide. Using these standards will improve the Agency's security posture and will permit us to leverage additional operations and business benefits while keeping our operations resources, maintenance and support costs at a minimum.

The standard will also improve:

- Access to and the sharing of information from a centralized location
- Centralized monitoring of all facilities from an Emergency Operations Center

FOR RFPS

- The operational and cost-effectiveness of adding a variety of modular features to the core systems, such as paging, e-mail, fire systems, facility management, etc.
- Alarm notification, response, and acknowledgement
- Operational flexibility for facility and Public Safety staff
- Single learning curve
- Reduce the cost for maintenance and system administration

8.2.2 Situational Awareness Platform Software

The Situational Awareness Platform Software (SAPS), is a software application that allows multiple, independently manufactured and installed security, life safety, and building systems to all interoperate under a single, common operating picture, giving a user access to information spreading across multiple systems as if they were all one single system. This "common view" is made even more valuable by the incorporation of powerful, rules-based tools within the SAPS system, which allows intelligent linking of seemingly unrelated events into "Situations" that represent patterns of activity that pose a threat to security or site-wide operations.

The SAPS objective is to monitor the identity and event data from the various systems, identify incidents and anomalies, and detect trends that could be a threat to our facilities. SAPS turns data into actionable intelligence when an incident is detected. SAPS have the capability to automatically alert the security operations staff and push the information to security control centers and first responders.

- Provide a software platform to enable integrating the various electronic systems across all agency sites
- Provide a single software perform solution for situational awareness.
- Provide a single system database for reports
- The SAPS will provide transparent notification of security related events for all agency security systems.

8.3 Communications Infrastructure Standards

The Port Authority Standard for Communications Infrastructure is Cisco. This applies to all future systems, as well as, upgrades to existing systems. This standard ensures the interoperability of all deployed systems and permits the full integration of systems into PAWANET. In addition, all Cisco equipment either designed in a low bid contract or specified in an RFP must be purchased through the Cisco Requirements contract, which is administered by TEC and permits the Agency to purchase equipment, maintenance and support services under the high discounts negotiated in the Requirements Contract.

This standard applies but is not limited to; Layer 2 and 3 Ethernet switches, Routers, Wireless Access Points (WAP), Mobile Access Routers (MAR), GIG E (Gigabit Ethernet) switching and networking and SONET (Synchronous Optical NETwork) equipment. Deviation from this standard requires the written consent of the CTO.

8.4 Server Infrastructure Standard

The Port Authority's standard platform for File & Print and Application servers is IBM.

Technology Department has contracted discounted pricing with our service provider for its servers and hardware support. In order for the agency to take full advantage of these savings, any new Application servers or File & Print servers must be built using IBM hardware purchased by TEC. This includes turnkey and distributed systems where File & Print or Application servers are specified in the design. Any replacement File & Print or Application servers must be IBM servers. Deviation from this policy will not be

FOR REFS

allowed without prior approval of the CTO or his designee.

9.0 Wireless Technologies

9.1 Wireless Standards

9.1.1 Purpose and Scope

This section references the standard policies and procedures for all wireless devices and technologies including voice and data capabilities that store, process, transmit or access data. This includes but is not limited to commercial and unlicensed wireless networks and laptops, cellular devices, scanning devices, messaging devices (email devices) and PDAs.

9.1.2 General Policy

Employees will only use PA owned wireless devices to store, process, transmit or access PA data.

9.1.3 Personal Area Networks - PAN

PAN technologies should not be used for transmitting information without encryption.

Bluetooth security alone is unacceptable because it is not encrypted and does not use Federal Information Processing Standardization (FIPS) 140-1/2.

9.1.4 Wireless Local Area Networks – WLANs

9.1.4.1 Overview

Business requirements have arisen throughout various Port Authority locations for the improved use of Wireless LAN technology to facilitate local user mobility. Research performed on the different technologies support the use of Cisco as opposed to various wireless vendors in an attempt to produce a standard that will provide the agency with a secure, robust and scalable solution as WLAN's continue to grow within the agency.

In summary, the current Port Authority Wireless LAN standards are based upon IEEE 802.11n draft 2.0 technologies. (802.11n is backwards-compatible with existing 802.11a/b/g network adapters.)

The physical infrastructure is now based upon a centralized WLAN architecture that relies upon Cisco wireless bridges, access points, mesh routers and newly implemented controllers. WLAN's should be standardizing on the 4404 and 4402 controllers at this time as described further in this document.

Wireless LAN technology is continually developing with rapidly evolving industry standards, government regulations, and vendor products. As a result, the WLAN Standard presented in this document will likely be superseded in the future as the technology and products change.

9.1.4.2 Scope

The scope of this document shall present some standards for the Agency Wireless LAN and the specification of all devices and configurations.

9.1.4.3 Principles

At the highest level, the principles for the Wireless Standard are based upon the following attributes:

- Security - use of strong encryption (e.g. WPA-TKIP / WPA2- AES) for use as authentication of all traffic on a port-to-port basis, with the use of credentials stored on a back-end RADIUS server utilizing key distribution.

FOR RFPS

- Scalability - with LWAPP access points & use of LWAPP tunnels
- Reliability - via authentication of users to the networking enterprise mode.
- Manageability - via secured ports and VPN / FW access.

9.1.4.4 Compliance Requirements

All specifications defined in this section may be effective upon approval of and complete concurrence with TEC's CTO, to update wireless standards and policies as per IEEE and Wi-Fi Alliance Standards

9.1.4.5 Device Specifications

The following sections will provide the various hardware components, and related firmware versions, that are specified for use in the Port Authority's WLAN solution.

9.1.4.6 Access Point (AP) Standard

Standards Details:

- 3600 AP's are the agency standard for WLAN deployment. These AP's have 802.11n 2.0 radios. Backward compatible to 802.11 a/b/g.
- 1310 AP/ Bridge is certified for use in unique situations where both internal and external antennae are supported. The major distinction is that of a more rugged chassis designed for higher-stress outdoor-type conditions. 3250 mobile routers for mesh deployments.
- AP Deployments will be Lightweight Access Point (LWAP)
- AP Standard Summary:
  - a) Two cables per pull during wiring for wired to wireless.
  - b) AP's & controller placements via RF propagation results.
  - c) PA supported standard AP's need to be verified with TEC
  - d) If wireless is primary connection-'load-balance' AP' cabling connection to two different network switches
- WLAN Controller Standard
  This standard is in the process of being upgraded to Network Control System (NCS) & Identity Services Engine (ISE) Appliance to accommodate more advanced wireless deployments.

9.1.4.7 Best Practice

The following information is industry best practices for wireless hardware implementation used for the Agency's deployments, not for wireless device configuration practices.

WLAN Best Practices Add-ons:

1. Ensure that the PA maintains an up-to-date wireless hardware inventory.
2. Identify rogue wireless devices via wireless intrusion prevention systems (IPS)
3. Enable automatic alerts on the wireless IPS
4. Perform stateful inspection of connections.
5. Augment the firewall with a wireless IPS
6. Mount AP in location that do not permit easy physical access
7. Secure handheld devices with strong passwords
8. Enable WPA and WPA2 under ENTERPRISE mode
9. Synchronize the AP's clocks to match networking equipment.
10. Manage remote physical locations of all access points which support an isolated network that needs access to PAWANET for server farms and internet access.
11. Maintain cryptographic strength range from 128-bits to 256-bits with matching symmetric algorithms AES-128 to AES-256

Wireless Control System (WCS):

FOR RFPS

1. Single license
2. Secure "WIRELESS LOCATION APPLIANCE" with real-time client tracking & RF fingerprinting
3. Secure Windows-Based deployment as minimum, for example, windows server 2003; intel dual-core; 3.2 GHz; 4-GB RAM; 80-GB hard drive; IPS devices; IOS firewall routing; HTTP port 80; HTTPS port 443.
4. Multi-homed server (i.e., two NIC cards)
5. Secure WCS and IIS (i.e ,internet information service), installation sequence
6. Create configuration group (configurate multiple controllers)
7. Secure auto provisioning with filtering
8. Secure WCS with RF modeling for heat map planning
9. Secure 15 second alarm summary refresh

9.1.4.8 Portable Electronic Devices (PEDs) – Cell Phones, PDAs, messaging devices, laptops and tablets

If a device receives information via a wireless technology, and that device allows that information to be placed directly into the corporate network at the workstation level, then all perimeters and host-based security devices have been bypassed. Therefore, the following procedures apply:

- PEDs connected directly to a PA wired network via a hot sync connection to a workstation is not permitted to operate wirelessly at the same time. Wireless solutions could create backgrounds into corporate networks.
- IR, Bluetooth and 802.11 peer to peer should be set to "off" as the default setting. Mobile code should be downloaded only from trusted sources over assured channels.
- Anti-virus software are required on devices and workstations that are used to synchronize/transmit data, if available. Where not available on a device, disable the synchronization capability or provide server or workstation based handheld anti-virus protection.
- PEDs are easily lost or stolen therefore approved file system/data store encryption software is required.
- PEDs need to be capable of being erased or overwritten to protect data. If the device is no longer needed and cannot be erased or overwritten, it must be physically destroyed.

9.1.4.9 Cellular and Wireless Email

Cellular and wireless e-mail devices are subject to several vulnerabilities (e.g. interception, scanning, remote command to transmit mode, etc). Therefore, the following procedures apply:

- Must have end-to-end encryption.
- PC based redirectors are not allowed as it requires the PC to be active at all times only server based redirectors will be used.
- The use of LANS and Wireless transmitters, i.e. Bluetooth etc. by PANYNJ personnel using PANYNJ equipment is strictly prohibited

9.1.4.10 Synchronization

Some synchronism systems will operate even if the workstation is locked and the wireless or handheld device is not registered with the sync application on the workstation. As long as the workstation is on, the user is logged on, the data application client (e.g. MS Outlook) is active, and the "hot sync" cable is attached to the workstation; any person can place a compatible wireless or handheld device in the "hot sync" cradle and download data. Therefore, the following procedures apply:

- "Hot sync" cable or cradle has significant security risks, therefore perform "hot sync", and then remove immediately once "hot sync" operation is complete.
- Secure "hot sync" cables and cradles.
- Use only PA approved third party sync access control software installed on all workstations.
- PA owned devices may only be synchronized with PA owned computer systems

FOR RFPs

9.1.4.11 Responsibilities of Technology Department

- Monitor and provide oversight of all PA wireless activities, insure interoperability of wireless capabilities across the agency.
- Develop appropriate technical standards for secure wireless and handheld solutions.
- Establish a formal coordination process to ensure protection of PA information with PA information systems employing wireless technologies.
- Review and evaluate wireless technologies, products, solutions that meet PA requirements.
- Identify approved monitoring mechanisms for wireless devices to ensure compliance with policy.
- Periodically review approved wireless technology standards and procedures to ensure products and solutions remain compliant.
- Support risk management activities associated with evaluating wireless services
- Act as central coordination point and final approval authority for any exceptions to this policy.
- Define or approve acceptable wireless devices, products, services and usage.
- Provide immediate consultation to PA units.
- Adhere to wireless procedures and standards, establish procedure for reviewing and approving requests for using wireless devices to store, process, or transmit information.
- Establish procedures for periodically reviewing approved wireless devices and services to ensure that the business requirement for device/service/system is still valid and meet current PA guidance.
- Establish procedures for inventory and control of wireless devices and equipment.
- Establish procedures and implementation plans for auditing wireless connections to the network.
- Provide user training.

9.1.4.13 Responsibilities of Wireless and Handheld Device Users

- Coordinate all requests through Technology Department…
- Read and follow standards.
- Access information systems using only approved wireless hardware, software, solutions and connections.
- Take appropriate measures to protect information, network access, passwords and equipment.
- Use approved password policy and bypass automatic password saving features.
- Use extreme caution when accessing PA information in open areas where non-authorized persons may see PA info (airport lounge, hotel lobby).
- Protect PA equipment and information from loss or theft at all times, especially when traveling.
- Keep current anti-virus software on devices.
- Use appropriate Internet behavior (e.g. approved downloads).
- Exercise good judgments in efficient cooperative uses of these resources and comply with current and future standards of acceptable use and conduct at all times.
- Report any misuse of wireless devices, services or systems to management.

9.2 Cellular Phone & Wireless Modem

The Port Authority obtains cellular service under governmental contracts. All orders for cellular service or equipment must be placed under these contracts. If the contract service provider cannot meet the requirements, a memorandum requesting approval to obtain cellular service outside of the contracts must be sent to the CTO.

9.3 Technology Mobile Device Policy

9.3.1 Introduction

Mobile devices are a class of handheld computers that currently offer limited functionality with compact size and portability. Additional functionality such as Word and Excel are already included in many Mobile devices, with further enhancements predicted.

FOR RFPS

In order to better serve the PA, and to limit the expense of supporting a wide variety of Mobile device hardware and software, Technology Department will support the use of the Windows and Apple IOS based devices.

With a Mobile device, a user can maintain their calendar, address book, to-do list, and e-mail on a platform that is very portable and easy to use. Integration with Outlook makes it possible for users to keep identical, synchronized copies of data on both the desktop application and the Mobile devices.

9.3.3 Software

The current version of Apple IOS software are supported.
Microsoft ActiveSync is used for connecting to the corporate E-Mail system.
Any software found to interfere with normal operation must be uninstalled in order to receive support from Technology Department.

9.3.4 Support

Support for Mobile devices hardware and software is provided by Technology Department through the Customer Support Desk. TEC will support the physical hardware connection (PDA cradle to PC) and software to support this connection. No software can be added to company owned mobile devices without TEC's assistance and CTO approval.

9.3.5 Training

Training will be available covering basic mobile devices use and integration with Outlook at the time of installation of the equipment. Training classes for the mobile devices may be provided in the future depending on user demands.

9.3.6 Acquisition

The PA will purchase Mobile devices for employees with a business need for the mobile device. Employees are responsible for obtaining management approval. TEC also recommends that a protective case (preferably a zippered case) be purchased to reduce damage to the units.
Since the PA owns the device, if an employee leaves the PA, the device is returned to the Director's office of their department.

9.3.7 Personal Acquisition

Employees, who purchase their own mobile devices, will not be allowed to connect to the PA corporate network or equipment, unless approved by Technology Department.
Customer Support Desk personnel will support all PA owned and authorized mobile devices.

9.3.8 Data Security Considerations

Users should carefully consider what type of information they store on their mobile. Extreme caution should be taken when using company confidential data on the mobile units.

All mobile devices accessing corporate resources are to be password protected.

9.3.9 Data Backup

Though it does not happen often, it is possible to lose or damage the data that resides in the mobile devices. Technology Department will provide assistance in attempting to recover files or data from data corruption.

FOR RFPS

Appendices

Appendix 1 -- Business Resumption Plan Document Format

I. PURPOSE

- Goals and objectives of plan
- Benefits obtained if plan properly implemented

II. SCOPE OF PLAN

- Planning assumptions
- Facilities and resources included in plan

III. NOMENCLATURE

- Recovery terms
- Definitions and acronyms

IV. DISASTER SEVERITY DEFINITION

Define level of potential disaster based on impact to critical functions. Explain what degree of operational disruption would constitute each level of disaster:

- catastrophic
- serious
- major
- limited

V. OPERATIONS RECOVERY PROCEDURES (Procedures for recovering services)

1. Indicate time frames in which essential operational/business functions must be resumed.

2. Specify sequence of operations recovery events and individuals responsible for activity. Note any specific activities required for particular levels of disaster severity. For example:

    - Notifications
    - Preliminary evaluation
    - Activate operations recovery personnel
    - Coordinate with emergency personnel
    - Evaluate recovery options and issue directive which details:
        - Assigned tasks
        - Project schedule/time frame
        - Coordination required
        - Identify relocation activities, if required
        - External/internal status updates

3. Identify items required for backup of critical functions. For example:

    - Alternate work site
    - Hardware/software

FOR RFPS

- Personal computers
- Necessary software packages
- Documentation
- Peripherals (printers, modems, etc.)
- Databases
- Emergency equipment
- Communications
- Transportation
- Supplies
- Security
- Operations and procedures manuals

VI. OFFICE/FACILITY BUSINESS SITE RESTORATION PROCEDURES

(Procedures for restoring physical facilities)

- Identify restoration responsibilities
- Assess damage
- Develop restoration plan/time frames

VII. BRP UPDATE PROCEDURES

- Specify responsibility for updating and communicating BRP changes
- Indicate frequency of review/update

FOR RFPS

Appendix 2 -- Communication Rooms/Closets Standards

SPACE
All data communication rooms must be designed with required and estimated space to meet immediate requirements, as well as, future growth.

ENVIRONMENTAL
The following conditions must be met:

a) Doorways/Entrances must be designed to support at least the minimum space requirements of 90”Hx72” Wx60” D.

b) The room’s cooling capabilities must be sufficient to support the heat dissipation requirements for the equipment. This requirement will be measured in minimum and maximum BTUs powered by AC-powered systems. Equipment specs will be supplied by TEC upon request.

c) Backup UPS systems are necessary to avoid equipment damage in case of site power failure.

d) Telco demarcs must be located in a central location with sufficient space to house Telco termination equipment.

e) The room should be designed with the appropriate fire safety regulations.

f) Cables trays must also be installed in the communications room ceiling where appropriate, to support the routing of data communications and Telco cables.

g) Basic 24”W/30”D/84”H cabinets with 19” racks must be installed to house communications equipment such as: routers, switches, hubs, DSUs/CSUs and monitors.

h) To create more wall space the use of wall mount racks can be installed, however, all wall cabinets must support rear access to the equipment. Appropriate sized plywood must be installed prior to mounting racks.

i) Category 5e/6 cable must be terminated in wall/rack mounted patch panel.

j) Fiber patch panel must be installed in fiber IDF panel with SC female interface.

k) The fiber must be neatly tie wrapped and enclosed in flexible inner-duct.

l) Telephone access must be installed in the appropriate location to provide for basic trouble-shooting and vendor support.

m) All communications equipment and cabinets must have ample room for easy access and proper ventilation.

FOR RFPs

Appendix 3 – Standard Cabling Schemes

a) Teflon-coated cables will be installed per fire code regulations.

b) Overhead cable trays and drop post must be installed for cable routing.

c) Cabling scheme must be used to label and identify all cables. All cables must be neatly tie-wrapped.

FOR RFPS

Appendix 4 -- Unified Wiring Plan

To satisfy existing and future voice and data communications requirements, while minimizing the need for wiring changes and additions, the Port Authority has adopted the following lateral wiring specifications for all workstations being constructed. This plan is applicable to all PA locations, except when specifically noted.

LATERAL CABLE:

Voice and data telecommunications requirements for each workstation will be provided by a combination of three individual cables, installed between the workstation and the serving telephone closet / intermediate distribution frame (IDF), in a "home run" configuration. All cabling installed will be of plenum type, fire retardant (FEP) rated.

Cable specifications:

(3) Cables capable of supporting Category 5e/6 capabilities as outlined in the TIA/EIA-568-B.2 standard. Specifically:

Gauge: 24 AWG Pair

Size: 4

Insulation: Plenum, fire code rating (FEP)

Cable allocations will be as following:

Cable #1: Voice**

Cable #2: Data

Cable #3: Data

- *100.0MHz is the speed the PA wants to deliver to the desktop.
- **Cable #1 is to be split in the workstation to support 2 telephones.

Technical specs for the Cat 5e/6 cable is as follows.

TECHNICAL DATA--ELECTRICAL				
	Horizontal		Patch	
Frequency MHz	Attenuation dB/100 m max.	Next dB min.	Attenuation dB/100 m max.	Next dB min.
1	2	62.3	2.4	62.3
4	4.1	53.2	4.9	53.2
10	6.5	47.3	7.8	47.3
16	8.2	44.2	9.8	44.2
20	9.3	42.7	11.1	42.7
31.25	11.7	39.8	14.1	39.8
62.5	17	34.3	20.4	34.3
100	22	32.3	26.4	32.3

FOR RFPS

TECHNICAL DATA--PHYSICAL			
	CMR	CMP	CM (Patch)*
Conductor diameter-in. (mm)	.020 (0.52)	020 (0.52)	024 (0.61)
Cable diameter-in. (mm)	.195 (5.0)	165 (4.2)	215 (5.5)
Nominal cable weight-lb./kft. (kg/km)	21 (31)	21 (31)	23 (34.2)
Max. installation tension-lb. (N)	25 (110)	25 (110)	25 (110)
Min. bend radius-in. (mm)	1.0 (25.4)	1.0 (25.4)	1.0 (25.4)
* Patch cables utilize stranded tinned copper conductors			

PARAMETRIC MEASUREMENTS		
	Horizontal	Patch
Mutual Capacitance	4.6 nF/100 m nom.	5.6 nF/100 m nom.
DC resistance	9.38 Ohms/100 m Max.	9.09 Ohms/100 m max.
Skew	45 ns/100 m max.	45 ns/100 m max.
Velocity of	72% nom. Non Plenum	72% nom.
Propagation	72% nom. Plenum	
Input Impedance	100 + 15% 0.7772-100 MHz	100 + 15% 0.772-100MHz
	ISO/IEC 11801	

COLOR CODE			TEMPERATURE RATING	
Pair 1	White/Blue	Blue	Installation	0 degrees C to +50 degrees C
Pair 2	White/Orange	Orange	Operation	-10 degrees C to +60 degrees C
Pair 3	White/Green	Green		
Pair 4	White/Brown	Brown		

FOR RFPs

Appendix 5 -- Telephone Closet / IDF Termination Blocks

Lateral Data cabling serving each workstation will be terminated on a CAT5e/6 patch panel (RJ45 face, 110 punch rear) in the telephone closet. For analog phone service, termination is to be on 110 blocks in telephone closet, allowing access to the telephone riser. For data, a patch cord is installed between patch panel and IT device. The patch panel can be mounted on the wall with a wall mount kit or in a rack if one is needed and should be appropriately numbered with the workstation number. The patch panel must be capable of supporting Category 5e/6 the TIA/EIA-568-B.2 standard. The patch panel shall have a swing away faceplate or rack mountable.

NOTE: The Category 5e/6 patch panel should be equivalent to the AMP SL series 110Connect Category 5e/6 patch panel or approved Category 6 patch panel. The number of ports may vary.

Each workstation shall be assigned a unique station identification number.

FOR RFPS

Appendix 6 -- Workstation Jacks

Workstations will be equipped with various components of the AMP Communications Outlet system (AMP equivalent can be used with TEC approval). Each workstation will be installed with (1) double-gang jack housing box and matching face plate, capable of securely mounting three Category 5e cables or Category 6 and four modular data connectors, maintaining the integrity of category 5e/ Category 6 capabilities as outlined in the TIA/EIA-568-B.2 standard. All workstation jacks will be wired in accordance with the TIA/EIA-568-B.2 standard. All modular jacks are to be labeled in accordance with TEC number schema.

FOR RFPS

Appendix 7 -- Standard Switches Inside the Department

Any switches in the following Cisco series are acceptable (Vendors will consult with the Technology Department (TEC) to determine the appropriate switch configuration at the time of proposal submission):

Cisco 3000 series – low capacity

Cisco 4000 series – medium capacity

Cisco 5000 series – medium capacity

Cisco 6000 series – high capacity

Cisco Nexus 7000 series – high capacity

Cisco Nexus 9000 series – medium and/or high capacity

FOR RFPS

Appendix 8 -- Workstation and Lateral Cable Identification Management

WORKSTATION AND LATERAL CABLE IDENTIFICATION/MANAGEMENT (Facility)

All lateral cabling installed to workstations at the Port Authority Facilities must be designated in accordance with the Port Authority's workstation and lateral cable identification code: This code consists of two elements, as follows:

1 - Room number or department name (acronyms are acceptable).

2 - Workstations (3 numeric digits)

The cable identification code for Workstation 10 in room 3801 at LGA CTB is 3801-010. The cable identification code for Workstation 15 in PA Automotive shop is Auto-015

FOR RFPS

Appendix 9 – Fiber Optic Specification for Network Services - PAWANET

General Scope of Work

1. Conduct a walk thru based on the specific Scope of Work for the job in question.
2. Note that all diagrams and or sketches that may be provided are approximates and not to scale.
3. All fiber optic cable is to be installed in rigid conduit or, where applicable, in plenum rated flexible inner duct.
4. Contractor shall furnish and install fiber optic cable as designated in the specific Scope of Work.
5. Fiber optic cable type for interoffice use shall be loose tube, with aramid yarn water block:
   - Singlemode Fiber – 8.3/125/250 micron diameter (core/cladding/coating) manufactured by General Cable or approved equal.
6. Fiber optic cable attenuation from the factory, before installation, shall not exceed:
   - Singlemode – 4db per km @ 1310nm/.3 db per km @ 1550nm
7. All fiber optic cable is to be labeled on each end and at any junction or patch panel with, 28 gauge, 2" wide embossed with ¼" high letters. The labels are to be fastened to the fiber optic cable using sealed wrap around labels or pliable Velcro ties.
8. Fiber optic cable shall be installed in accordance with the manufacturer's specifications. Any portion of the cable damaged during installation will be repaired or replace by the contractor without any additional cost to the Port Authority of New York New Jersey.

Fiber Optic Terminations

1. Fiber optic terminations will use **SC** connectors unless otherwise specified in the Scope of Work.
2. Fiber optic terminations shall not yield more than 1db per mated (at the bulkhead) connector.

Fiber Optic Testing

1. Fiber optic testing shall be performed by the contractor and certified fiber optic technicians.

Fiber optic technicians will be prepared to complete test procedures with the following equipment:

- Source and power meter testing to provide optical loss measurements.
- Reference test cables and mating adapters that match the cables to be tested.
- Cleaning materials – lint free cleaning wipes and pure alcohol.
- OTDR test set with the proper launch cables and adapter types.
- Power loss testing from both ends.

2. Fiber optic technicians will perform OTDR test on all terminated fibers unless otherwise noted in the Scope of Work.

3. Fiber optic test results shall be recorded, and reports provided to the PA in hardcopy and via a readable txt file (PDF or RTF is acceptable).

FOR RFPs

Appendix 10 -- Public Telephone Ordering Standards

Technology Department (TEC) staff is responsible for the management of the permit for public telephone service are available to answer any questions and provide direction for any matter relating to public telephones.

General Standards

All public telephone requests – that is both coin and non coin in any Port Authority space or any area of the tenant space – both "public" and "club" locations will be coordinated by the Port Authority to cover both New York and New Jersey.

Process

When the Facility, Property Manager, tenant or their representative (e.g. designer, architect, general contractor) has a public telephone requirement, they will contact the Technology Department (TEC) whom will review the request and provide coordination with the appropriate service provider.

FOR RFPS

Parking Access and Revenue Control System—Design, Installation & Maintenance

Attachment L
Computing Resources Policy

AI 15-4.03

Office of the Executive Director

Revised: April 6, 2012

COMPUTING RESOURCES

I. Introduction

A. Computing resources provide the Port Authority with significant benefits in productivity and efficiency. The provision of computing resources is intended and designed to facilitate the official business of the Port Authority. Port Authority rules and regulations that govern the responsibilities of employees apply to employee use of computing resources. This Instruction is intended to clarify and ensure that computing resources are used in a professionally responsible manner and appropriate steps are taken to safeguard the confidentiality, integrity and availability of business systems, data and equipment.

B. For purposes of this Administrative Instruction, computing resources include, but are not limited to, personal computers, software, peripherals, data storage and devices, personal digital assistants, local and wide area network components, Port Authority provided connections, E-mail, internet access, laptops, terminals, remote access and any other means of automated information exchange or data access.

II. Instruction

A. Computing resources provided to employees and other authorized persons are Port Authority property and intended for Port Authority business. Computing resources are not to be used for personal gain or in support of any purposes not related to Port Authority business. Because the use of computing resources is both extensive and an efficient and convenient method of communication and data processing, it is understood that there may be incidental personal and non-commercial use of these resources. Such incidental use is subject to this Instruction, and authorized users are expected to use prudent judgment to ensure that all computing resources are used for the intended purpose of Port Authority business.

B. When necessary for official or business purposes, the Port Authority reserves the right to monitor and/or log all computing activity. Requests for monitoring will be made to and authorized by the Executive Director in writing and only then for limited justified and reasonable cases. Further,

the Port Authority reserves the right to inspect computer resources to ensure that actual use is consistent with this Instruction. The Port Authority may use data, logs, diaries, and archives in accordance with its normal business practices and instructions (including compliance with requests from appropriate legal and regulatory authorities and agencies) and for adherence with this Instruction.

1. The Port Authority, through supervisors or other management employees authorized in writing by the Executive Director only, may access or monitor a user's assigned computing resources with justifiable reason.

2. The Port Authority may inventory and inspect all data storage devices and other computing resources for the sole purpose of ensuring their continued proper maintenance and operation.

C. Depending upon content, data stored within computing resources may constitute records of the Port Authority and the organizational data retention schedules (Record Retention Manual) and instructions on access to such data (the Freedom of Information Policy) are applicable. However, users should be aware of the limited retention period for e-mail messages described in Par. IV of the Instruction.

D. Directors are responsible for implementation of this Instruction within their departments.

III. Procedures

A. Passwords

1. Users should be aware that the existence of individual confidential passwords does not suggest that computing resources may be used for personal confidential purposes, or that any data or information is the property of the individual user or is personally confidential.

2. Employees are responsible for maintaining the confidentiality of passwords and may be held accountable for use of computing resources in their name accessed with their password.

3. Passwords should be difficult to guess and changed at least once every 90 days or in accordance with information system standards.

B. Usage Requirements

1. Authorized users of Port Authority computing resources, when communicating with others, are required to:

a. Identify themselves honestly, accurately and completely.

b. Maintain a professional demeanor.

c. Protect Port Authority data from unauthorized use or disclosure.

2. At all times, authorized users must respect the legal protection provided to programs and data by copyright and license.

C. Prohibited Uses

1. Authorized users of Port Authority computing resources may not utilize them:

a. For transmitting, retrieving, creating, viewing, displaying or storing any pornographic, harassing, threatening, abusive, defamatory, obscene, or sexually explicit materials or materials which contain ethnic slurs or racial epithets, or which generally disparage others based on race, national origin, sex, sexual orientation, gender identification, age, disability, religious beliefs, or political affiliation, or which contain other unlawful material.

b. To transmit confidential, proprietary or business sensitive information.

c. To interfere with or disrupt network users, services or equipment either within the Port Authority or on the Internet.

d. To access other computing resources without authorization or attempt to circumvent authorization procedures or controls.

e. For private purposes such as marketing or business transactions.

f. For religious, political or outside business purposes.

g. For unauthorized not-for-profit business activities.

h. For advertising of products or services.

i. For personal gain.

j. To obtain or utilize unauthorized entertainment software, music or games.

k. To permit access by unauthorized users.

l. To send material in violation of the copyright.

m. For solicitation of funds.

n. For employee organization business.

2. Electronic mail practices such as “spamming” (unauthorized mass mailings to Port Authority employees or external recipients or postings to bulletin boards), hostile communications, “chain letters”, “spoofing” (taking the identity of another person for the purpose of concealing one’s own identity), or knowingly transmitting software containing harmful components such as a virus, are prohibited.

3. Allegations of misuse of computing resources may be made to supervisors or managers, consistent with existing Port Authority instructions applicable to misuse of property or improprieties or inappropriate or illegal behavior in the workplace.

IV. Retention of Electronically Stored Data

A. E-mail messages are generally of short-term import and should be discarded routinely. E-mail is automatically deleted from a user’s mailbox and backup storage 120 days from the date of receipt or creation, without notice.

1. Depending on the content of the message and/or its attachments, it may be desirable to retain the information for longer periods. Such messages or attachments should be stored on local or server drives as necessary.

2. As suggested in Par.II.C., depending on the content of the message and/or its attachments, care and consideration should be given as to which documents should be retained based on the appropriate record retention schedules.

B. Users should take appropriate steps to ensure that important Port Authority data other than e-mail is backed up in case of equipment failure. This includes data stored on Port Authority computing resources in the office and, where authorized, at home. Data stored on shared devices which are part of the Port Authority’s enterprise wide network system are backed up and retained for a period of time in accordance with standards issued by the Port Authority.

C. Users should also be aware that deletion of an e-mail message or attachments or other data may not automatically delete the message from

electronic storage devices. The data may continue to reside in the user's local or network drives, or may be stored in backups of the system.

V. Applicability to Employees and Other Users

A. This Computing Resources Instruction applies to all employees, volunteers, contractors, supplemental staff, consultants, and other individuals who are provided access to any or all Port Authority computing resources.

B. Employees

1. Employees of the Port Authority (or its subsidiaries) whose employment is terminated or suspended have no right to access any Port Authority computing resource, including Internet access and e-mail accounts and content.

2. The misuse of computing resources privileges may subject the employee to disciplinary action in accordance with Port Authority rules, and/or other applicable rules or laws, and may be grounds for loss of such privileges, dismissal from employment, or other administrative action. In addition, violations of this Computing Resources Instruction or other misuse of computing resources may be referred for criminal prosecution.

C. Non-employees

1. Third parties (i.e., individuals who are not employees of the Port Authority or its subsidiaries) should only be provided access to Port Authority computing resources as necessary for the business purposes of the Port Authority and only if they comply with all applicable rules.

2. Non-employees who are in violation of the provisions of this Computing Resources Instruction will be removed from access to all Port Authority computing resources. In addition, other legal remedies, civil (including contract revocation) or criminal, may be pursued.

DISCLAIMER

Although issued in revised format, the information contained in these Administrative Instructions (AIs) reflects the content of previously issued Administrative Policy Statements (APs) and, in certain limited instances, Port Authority Instructions (PAIs). The rules set forth in these AIs will remain in effect until changing conditions require their revision. This body of instructions is not intended to be exhaustive with respect to all the responsibilities of employees and it does not constitute a contract. These AIs will be updated from time to time to reflect changes or additions as appropriate, at the direction of the Executive Director.

Parking Access and Revenue Control System—Design, Installation & Maintenance

Attachment M
Cyber Security Guidelines for the Port Authority of NY & NJ

CYBER SECURITY GUIDELINES FOR THE PORT AUTHORITY OF NY & NJ

V 3.4

Prepared by: Technology Services Department (TSD)

As of August 15, 2011

Table of Contents

Introduction 3

1. User Authentication 3

a. User Accounts 3

b. Password Authentication 3

2. Information Assurance 4

a. Computer Devices (Desktops, Laptops, CAD Workstations) 4

b. Mobile Computing Devices 5

c. Servers 6

d. Virtual Environment 6

e. Portable Media 7

g. Cyber Scrubbing 8

3. Data Center 8

4. PAWANET 9

a. Network Devices 9

b. Firewalls and Intrusion Detection Appliances 10

c. Proxy Service 11

d. Remote Access (Client-to-Site) 12

5. Virtual Private Network (VPN) (Site-to-Site) 13

6. Internet Access 14

a. Outbound Traffic Requests 14

b. Inbound Traffic Requests 14

7. E-Mail 15

a. E-Mail Hosted Environment 15

b. E-Mail Virus and Spam Protection and Content Scanning 15

8. Desktop Patch Management 16

9. Server Patch Management 16

10. Content Management 16

Introduction

The Port Authority significantly relies on Information Technology (IT) to support its various businesses and achieve its strategic mission. To ensure that information and systems are safe, the Technology Services Department (TSD) has developed a formal IT Security Program and Cyber Security Guidelines, focused on protecting the Agency from all types of security threats to the Agency's IT infrastructure.

The Cyber Security Guidelines encompass all systems, automated and manual, for which the Agency has administrative responsibility, and identifies measures taken to protect a network, system, computer device, etc., against unauthorized access or attack.

1. User Authentication

a. User Accounts

i. The Agency uses the Request for Access to Information Systems (Form PA 3624A), which can be found online on ENet, for all user account and systems access adds, changes and deletions. The form is submitted by a Port Authority employee and is approved by the departmental approver.

ii. Upon approval from the department, the form reaches TSD and is reviewed by TSD for approval or denial.

iii. If elevated rights (i.e., Administration Rights) are requested with expiration date identified, Assistant Director of Technology Infrastructure approves; if requested not to expire, Director of TSD approval is required before processing.

iv. Both Daily and Weekly personnel additions and terminations are forwarded to TSD. TSD ensures that 3624A's exist, or are processed for, each change. Submission of personnel transfers, however, are the sole responsibility of the Business Manager.

v. All users accessing the Port Authority's network must authenticate to the Agency's Directory Services. Directory Services is a database containing descriptions of all network devices including servers, printers, shared devices and user accounts.

b. Password Authentication

i. A "strong" password should be created:
   1. User accounts should be changed every 30 days; You must change every 90 days
   2. Administrator accounts must be changed every 30 days
   3. At least eight characters is preferred; Six characters is the minimum
   4. Should include both alpha and numeric characters
   5. May include at least one special character
   6. May include both upper and lower case letters
   7. Cannot reuse password within a one-year period

ii. Accounts on servers, desktop and laptops are locked after five (5) unsuccessful login attempts. Accounts on BlackBerry devices are locked after ten (10) unsuccessful login attempts.

iii. Initial password for systems and applications access should be changed on first login and may only be changed once a day.

iv. Never write it down
v. Never share it
vi. Cannot be stored in clear text
vii. Cannot be stored in an automated logon process (e.g., macro, application code, etc.)
viii. Notify the Customer Support Desk, 10-7469, immediately if you suspect your password has been compromised

2. Information Assurance

Downloading and printing Confidential Information carries with it the responsibility to protect that information in accordance with the requirements of the Agency's Information Security Handbook (http://eNet.panynj.gov/home/pdf/Corporate-Information-Security-Handbook.pdf). In addition, possession of electronic files containing Confidential Information assumes full responsibility for the proper handling, storage and transmittal of this type of information in the same manner as hard copy requirements.

Users who possess electronic files containing Confidential Information shall adhere to the following guidelines to maintain the proper protections of this material.

Electronic equipment that has a storage device or persistent memory, such as desktop computers, laptops, CAD desktop computers, portable computing devices (e.g., BlackBerry devices) must adhere to the following guidelines to maintain the proper protections of this material.

a. Computer Devices (Desktops, Laptops, CAD Workstations)

i. All computing for the Agency is performed on PA approved computer devices. To protect them against viruses and malicious software, (e.g., Trojan Horses), McAfee VirusScan Enterprise & AntiSpyware is installed. In addition, software restriction policies are fully integrated with Active Directory and applied on all computer devices to prevent unauthorized installation of non-standard applications. Agency approved software, which can be found on the TSD Department eNet site, is installed by TSD. Each Line Department is responsible for maintaining a current inventory of their approved Line Department specific software licenses and for providing proof of license to the TSD at time of installation request.
ii. TSD oversees the System Administration and day-to-day operational support for PA approved computer devices.
iii. The automatic lock/screen saver feature will activate after a period of fifteen (15) minutes of non-use.
iv. TSD maintains a "chain of custody" process surrounding all hard drives. Currently, all removed hard drives are managed and stored off-site at a secure location. Required exceptions are in place with the Office of the Inspector General (OIG) and Public Safety (PSD).

v. User Responsibilities:
    1. Individuals granted access to the Port Authority's network or information systems shall secure computer devices from unauthorized access.
    2. When leaving a computer device unattended, users should apply the *"Lock Workstation"* feature (Ctrl/Alt/Delete, Enter).
    3. Unattended computer devices should be secured from viewing by password protected screen savers.
    4. Confidential Information must be stored on a networked drive directory rather than the computer device's hard drive. (Note: Due to the nature of the functions of the Office of Inspector General [OIG], there will be occasions when OIG must deviate from this practice.)
    5. Computer devices and monitors should be turned off at the end of each workday.
    6. Users must not disable or alter security safeguards (e.g., virus detection software) installed on the PA approved computer device.
    7. Users must not load non-Agency software or proprietary non-Agency data onto an Agency owned computing device.

b. Mobile Computing Devices

i. All mobile computing resources (e.g., laptops, BlackBerry devices, mobile phones, etc.) and information media must be secured to prevent compromise of confidentiality or integrity while on or off Agency premises. Information contained on these mobile computing devices is governed by the Information Security Handbook (ISH).

ii. Personal Mobile Computing Devices are not allowed to connect to the Agency's corporate network or infrastructure, unless pre-approved by the Director of TSD.

iii. To protect data information and hardware, a password is required on every BlackBerry device. An inactivity timeout value is set to lock the device after 30 minutes of inactivity.

iv. TSD maintains a "chain of custody" process surrounding all hard drives. Currently, all removed hard drives are managed and stored off-site at a secure location. Required exceptions are in place with the Office of the Inspector General (OIG) and Public Safety (PSD).

v. User Responsibilities:
    1. Care must be taken when using mobile computing devices in public places, meeting rooms and other unprotected areas outside of the Agency's facilities. Protection must be in place to avoid the unauthorized access of information stored and processed by these devices. *Please contact TSD to discuss protection measures if you identify a device/scenario meeting such criteria.*
    2. It is important that when such devices are used in public places, care must be taken to avoid the risk of unauthorized persons viewing information on the screen.
    3. Mobile computing devices must be physically protected against theft, especially when in transit (e.g., car, train, plane, etc.) or at rest (e.g., hotel rooms, conference rooms, etc.).

4. Equipment carrying important, sensitive and/or critical information must not be left unattended and must be physically locked away and secured.
5. Mobile computing devices must not be checked in airline luggage systems. These devices must remain in the possession of the Port Authority employee at all times.
6. By default, Wireless Detection (e.g., Bluetooth, WiFi, Wireless Networks, etc.) must be turned off on all mobile computing devices, *unless* it is required. Only when required should the Wireless Detection be turned on for use. Once completed, the Wireless Detection should be immediately turned off.
7. Users must not load non-Agency software or proprietary non-Agency data onto an Agency owned computing device.

c. Servers

i. The standard for general purpose Application servers, Database servers and File and Print Computing is IBM. Microsoft (MS) Windows 2003 and 2008 R2 64-bit Server (Standard and Enterprise) are the supported Operating Systems for these servers.

ii. Fault Tolerant Application servers and Database servers is NEC FT. MS Windows 2003 and 2008 R2 64-bit servers are the supported Operating Systems for these servers.

iii. Operating system settings and configuration will be performed by TSD to ensure compliance to appropriate security policies based on server roles, e.g., Web, Database, Fax, etc..

iv. All servers and communication equipment must be located in access controlled/locked rooms (or secured with a cable and lock at the very least), in data cabinets with dual power, with the keyboard secured to prevent tampering and unauthorized use, with appropriate environmental cooling and monitoring oversight.

v. TSD maintains a “chain of custody” process surrounding all hard drives. Currently, all removed hard drives are managed and stored off-site at a secure location. Required exceptions are in place with the Office of the Inspector General (OIG) and Public Safety (PSD).

d. Virtual Environment

i. All ESX servers and associated storage components must be located in access controlled/locked rooms (preferably the Agency Data Center environments), in data cabinets with dual power, with the keyboard secured to prevent tampering and unauthorized use, and with appropriate environmental cooling.

ii. All ESX server implementations must implement a management framework consistent with our PA ESX Administration Guide, which from time-to-time will be updated to reflect Standard Operating Procedures.

iii. All ESX server implementations must provide “as built” documentation consistent with the framework established in our VMware Infrastructure Documentation For the Port Authority. This document must be kept current as changes to the environment are implemented.

iv. All ESX server implementations (i.e., ESXi Operating System) must be patched on a regular basis using the management framework established in our PANYNJ ESX Patch Management document, which from time-to-time will be updated to reflect current patching procedures.
v. All ESX-based Guest Virtual Machines must implement Operating System configurations and security settings, consistent with those identified in the Standards and Guidelines, System Administration and Windows Server Installation documents.
vi. Access to ESX Operating System must be limited to System Administrators who have received ESX training and certification in the appropriate VMware components.
vii. Storage Devices or Storage Area Network (SAN) should be configured based on ESX implementation purpose/application needs:
    1. Switch Zoning and/or Volume Partitioning – used to separate servers/storage based on the functionality and/or data criticality.
    2. SAN-to-SAN Replication – used to provide extra level of protection and high availability for mission critical data by block level replication between physical locations.

e. Portable Media

The risk of unauthorized disclosure of highly sensitive data is very high when such data is stored on individual-use electronic devices (e.g., flash drives, portable hard drives, DVDs, CDs, memory cards, etc.) and media, as these items are easily stolen or misplaced.

i. Personal portable media devices are not allowed to connect to the Agency's corporate network or infrastructure, unless pre-approved by the Director of TSD.
ii. It is important that portable devices offer strong protection, e.g., hardware encryption. Additionally, the encryption key must be protected with strong user authentication. *Please contact TSD to discuss protection measures if you identify a device/scenario meeting such criteria.*
iii. The Agency strictly limits the circumstances under which highly sensitive data may be stored on these individual-use electronic devices and electronic media. It further mandates that strict security requirements be met when highly sensitive data must unavoidably be stored on individual-use electronic devices or electronic media. *Please refer to the Agency's Information Security Handbook (http://eNet.panynj.gov/home/pdf/Corporate-Information-Security-Handbook.pdf).*
iv. User Responsibilities:
It is the responsibility of individuals to determine if they have sensitive data on their device(s) and/or media, and, if so, to ensure compliance with the following guidelines:
    1. The Director of the Department with which the individual is primarily affiliated must state, in writing, that such storage is an essential business need and must file the written statement and approval in a secure location for subsequent audit purposes. The Department Director must also ensure the individual has a signed Electronic Access Agreement on file with TSD.

2. Highly sensitive data must be securely encrypted on the individual-use electronic devices or electronic media according to encrypted methods recommended by TSD. Login password must be enabled for the individual-use electronic device, and if available, the electronic media. The password must meet or exceed appropriate complexity levels stated by the Agency. The password must not be shared with anyone.
3. The data must be deleted from the individual-use electronic devices or electronic media as soon as it is no longer required, using secure methods according to the Agency's Information Security Handbook.
4. Management of the individual-use electronic devices or electronic media may not be outsourced to any party external to the Agency without written approval from the Director responsible for the department with which the individual is primarily affiliated.
5. All individual-use electronic devices and electronic media should be stored in a secure location or locked cabinet when not in use.
6. Users must not load non-Agency software or proprietary non-Agency data onto an Agency owned computing device.

f. Centralized Data Backup
Approved standard software products are used to perform centralized and scheduled server backups, to be managed automatically, logged and stored remotely with encryption.
   i. The backup strategy for servers connected to the Port Authority network (PAWANET) reflects the intent to protect data, files and electronic records stored on these servers in the event of data loss or corruption.
   ii. Media containing backed up data is stored off-site at a secure location, to be retrieved for disaster recovery purposes, if required.

g. Cyber Scrubbing
   i. On a file-by-file basis, Cyber Scrubbing may be used to permanently delete Confidential Information only in accordance with the Port Authority's Records Retention Policy.
   ii. Once contacted, TSD will utilize the CyberScrub suite of software to remove Confidential Information as requested.

3. Data Center

i. Located in a gated campus that controls access via numerous layers of physical and electronic security devices.
ii. Protected with fire safety system, leak detection system and is equipped with fully redundant backup systems for communications, power and cooling infrastructure.
iii. Threat and risk assessment reviews and audits of security standards, operating procedures, and other protective measures are performed regularly to ensure we provide a secure, reliable and available centralized information systems environment to house the Agency's information and computing equipment.

4. PAWANET

The Port Authority has a modern distributed computing network, which is managed as an Enterprise resource. The network connects all individual computing devices, servers, printers and other devices in a unified computing infrastructure that makes it possible for the Port Authority to conduct its business. Please also reference the TSD Standards and Guidelines document, from the TSD eNet Home Page, for additional detailed information.

a. Network Devices

i. All users accessing the Port Authority's network must authenticate to the Agency's Directory Services. Directory Services is a database containing descriptions of all network devices including servers, printers, shared devices and user accounts.

ii. Access to network devices such as routers and switches is limited by the use of Access Control Lists (ACLs). Access to network routers and switches is authenticated by Cisco's TACACS (Terminal Access Controller Access Control System).

iii. The SNMP V3 (Simple Network Management Protocol) Security Feature has been applied to all routers and switches to deny unauthorized access.

iv. All router and switch configurations are updated regularly based on the Cisco Security Best Practice policy. This policy, as well as the PA Standard Configuration policy, is available upon request.

v. Modems and wireless devices must be pre-approved by the Director of TSD and follow all security and encryption best practices referenced within and in the TSD Standards and Guidelines.

vi. Penetration tests are conducted twice a year.

vii. The Enterprise Network consists of the PAWANET and connected Local Area Networks (LANS). The line of demarcation between the cable and wiring, which is the responsibility of the carrier, and the Port Authority's area of responsibility, is usually a secure limited access wiring closet. The Port Authority's Enterprise Network consists of the following components on the Port Authority side of demarcation:

1. Enterprise Devices
    a. Cabling (both copper and fiber optics)
    b. Routers
    c. Switches
    d. Wireless Access Points (WAP)
    e. Wireless Bridges
    f. Fiber Optic SONET Nodes
    g. Wiring Closets
    h. Communications Equipment Racks
    i. Server Racks
    j. Servers
    k. Storage Area Networks (SAN)
    l. Network Printers
    m. Video Encoders and Decoders

2. LAN Devices
    a. Workstations (Desktops and CADS)
    b. Laptops
    c. Local Printers
    d. Scanners
    e. Copiers
    f. PC Peripherals
    g. VOIP (Voice Over Internet Protocol) Telephones
    h. Voice Analog Gateways
    i. Cameras
    j. Security Card Access Devices

b. Firewalls and Intrusion Detection Appliances

i. The Agency uses several layers of stateful inspection firewalls to control traffic between the PAWANET, Public and Private DMZs, directly connected vendors and the Internet. In addition to stateful inspection, the firewall technology offers application intelligence, which allows for deeper protocol-specific traffic inspection and protection against IP spoofing, Denial of Service (DoS) and other kinds of attacks. The access is controlled by policy sets, which limit the source, destination, port, protocol and in some cases, certain functionality of the protocol. The traffic that is not explicitly allowed is denied. Both allowed traffic and denied traffic are logged. The rule usage is reviewed on a periodic basis.

ii. The Agency uses a multi-layered network-based Intrusion Detection (IDS/IPS) solution to protect the perimeter against intrusions. The updated attack signatures are automatically downloaded from the vendor's repository on an hourly basis and are automatically applied to the intrusion prevention system units. The IPS architecture allows for the centralized mining of the events across multiple IPS nodes and email-based alerts for high-priority events. Events are monitored and correlated on a regular basis. Correlation is also performed between the application protection policy of the firewall and the IDS layers of defense.

iii. Host-based Intrusion Detection (HIDS) is installed and activated by TSD based on the purpose and physical location of the server. The technology protects the host against network attacks by examining incoming and outgoing traffic as well as the events on the host. The technology has the same log management and email alerting functionality as network-based intrusion detection. Events are monitored and correlated on a regular basis.
    1. Examples include:
        a. Servers having a legal/regulatory obligation to ensure their security.
        b. Servers housing information, that if disclosed, could pose a security threat.
        c. Servers supporting a business process that must be available 24 x 7, such as physical access control.
        d. Servers that are accessible to the outside world, firewalls, VLANs enforcing internal zone/domain separation.

iv. All layers of perimeter security appliances offer several layers of intra-site and inter-site redundancy with automatic failover. The performed capacity planning and gathered experience over multiple years of maintenance guarantee seamless failover and adequate capacity of the remaining system to provide full functionality and no performance degradation in case of scheduled or ad-hoc failover.

v. In the event of a security perimeter breach and/or the internal networks being compromised, the intrusions will be reported to the Office of the Corporate Information Security Officer and the Office of the Inspector General. We will retain the applicable logs from the perimeter security devices bearing the details of the perimeter breach.

c. Proxy Service

The proxy appliances and services offer extensive management, monitoring and reporting capabilities.

i. The Agency has deployed multi-layered Web security appliances from one of the leading security vendors. The appliance performs the following tasks:
   1. Allows authenticated users to access Internet sites in accordance with the access policy
   2. Caches frequently used content
   3. Performs filtering of the malicious and inappropriate Web sites based on:
      a. Site Database
      b. Reputation Database
      c. Proximity Vector
   4. Reputation Filters in place analyze more than 200 different web traffic and network-related parameters to accurately evaluate the trustworthiness of the course of the Web content.
   5. Performs deep application content inspection of the request and return traffic with several anti-virus and anti-malware engines. The solution employs sophisticated object parsing and streaming techniques as well as hardware optimization and acceleration to enforce security policies.

ii. All device databases are being continuously and automatically updated with the new content via subscription service. The subscription service taps into the vendor's security event and signature database, which is updated by the 24/7 security team and cross-correlated with the events across the Internet. Such an approach allows for protection against the attacks that were initiated across the globe but have not yet spread to North America (including time-dependent outbreaks of viruses).

iii. The proxy appliances provide hourly, daily, weekly and monthly statistics of the vital usage and performance parameters, which are stored on the appliances and periodically mailed to the members of the maintenance and management team. The technology also comes with the management application that allows for log consolidation and log mining on a separate server. The access logs are profiled on a regular basis and mined for specific usage per request of OIG and/or Public Safety representatives to assist with internal investigations.

d. Remote Access (Client-to-Site)

i. Infrastructure

1. The Port Authority corporate Remote Access System (RAS) provides authorized users with access to the Port Authority network resources and applications.
2. Access to a number of Port Authority public servers is protected either by a secure reverse proxy solution or by a managed VPN solution, each of which requires user authentication against Directory Services as well as masks the internal address space of the corporate network and the DMZ infrastructure.
3. The operating system of the Port Authority servers is hardened with all unneeded services being disabled.
4. Administrative access to the server is encrypted with SSL/TLS certificates.
5. All servers are monitored by a central monitoring server which generates E-Mail notifications when problems are discovered.
6. Server and application access logs are collected and processed on a regular basis.
7. Both the OS and the applications are patched with the most recent service packs and hot fixes on a scheduled basis. In the case of virtualized servers, the underlying host OS is also patched and secured.

ii. VPN Access

1. Remote access from external sources (such as a user's home) is achieved through an Internet-based managed VPN service.
2. It utilizes client software and proprietary hardware and software.
3. The servers are located at each of the Agency's secured Data Centers.
4. Requests for remote access are handled via the Request for Access to Information Systems (Form PA 3624A), which can be found online on ENet.

iii. Agency Application(s) Access

1. Single sign-on and remote authentication services to access internal web-based applications from the Internet have been established.
2. Identity-based Web security service and a two-form factor secure authentication device are required for authorized users to securely authenticate to the network over the Internet.

5. Virtual Private Network (VPN) (Site-to-Site)

Because the Internet is inherently insecure and provides no security mechanisms, dial-up access to the Internet is prohibited from any device that is attached to any part of the Agency's PAWANET Network. This includes accounts with third party Internet service providers. Users will not use the Agency's Internet accounts to establish connections to these third party services, unless authorized in advance to do so by the Agency's management and the security of the connection is reviewed and approved by the Director of TSD.

i. The Director of TSD must approve all other connections from PAWANET to external networks, in advance. Connections will be allowed only with external networks that have been reviewed and found to have acceptable security controls and procedures, or where appropriate security measures have been implemented by the Agency to protect the Agency's resources. All connections to approved external networks will pass through an approved Agency firewall and intrusion detection sensor. Remote access to PAWANET and resources will be permitted provided that authorized users are authenticated, data is encrypted across the Internet and privileges are restricted.
ii. External networks must adhere to the PA Standard Configuration policy, available upon request.
iii. Audit trails and system logs for external connections will be reviewed weekly. The Network Manager will require the business managers to validate the need for all such connections on a quarterly basis. When notified and confirmed in writing, to both the business manager and the Director of TSD that the need for connection to a particular network is no longer required, all accounts and parameters related to the connection will be deleted within one working day.
iv. Any connection between firewalls over public networks must use encrypted Virtual Private Networks (VPNs) to ensure the privacy and integrity of the data passing over the public network. All traffic emerging from the VPN tunnel should pass through the layers of firewall and IDS/IPS traffic inspection. The Director of TSD, prior to implementation, must approve all VPN connections. Appropriate means for distributing and maintaining encryption keys must be established prior to operational use of VPNs.

6. Internet Access

a. Outbound Traffic Requests

i. The Agency encourages authorized employees to use the Internet for appropriate Agency business use. They offer valuable resources for employees and provide business value to the Agency. However, some web sites contain material whose content is clearly inappropriate for anyone using the Agency's resources. Therefore, access to inappropriate sites from Agency's computing devices is disabled. Such sites include: sexual content, violence, weapons, hacking, drugs, etc.

ii. Misuse of Agency resources will not be tolerated. All Agency Employees and Non-Employees are responsible to follow the requirements outlined in Agency's Computing Resources Policy (http://eNet/resources/ai/ai15403.pdf). Examples of behavior that could result in disciplinary action include use for:

1. Personal gain or profit
2. Spoofing (representing yourself as someone else)
3. Copying or posting the Agency's or third party's information without permission
4. When it interferes with the operation of the Internet gateways
5. Unauthorized attempts to break into any computing system whether the Agency's or another organization's
6. Theft or unauthorized copying of electronic files
7. Posting sensitive Agency information to unauthorized personnel
8. Creating or forwarding chain letters
9. Personal communication using "instant messaging" or similar technology
10. Downloading or uploading malicious code
11. Downloading or uploading inappropriate material for "sniffing" (i.e., monitoring network traffic); except if authorized as job responsibilities

iii. Internet usage is monitored through use of proxy logs and reviewed with the Director of TSD on a monthly basis.

iv. Outbound traffic is provided via both FTP (File Transfer Protocol) and SFTP (Secured File Transfer Protocol).

b. Inbound Traffic Requests

i. Access to the PA-hosted Web sites in the DMZs is regulated by the firewall rules, which deny all traffic that is not explicitly allowed.

ii. The access to the PA-hosted Web sites is further controlled by the several layers of IDS/IPS technology and by host-based intrusion detection running on the host (as described in Outbound Traffic Requests section).

iii. High priority events generate E-Mail based alerts to the TSD perimeter security team.

iv. Inbound traffic is allowed over SFTP (Secured File Transfer Protocol) from specific IP addresses. The data must be encrypted.

7. E-Mail

a. E-Mail Hosted Environment

i. The Port Authority E-Mail environment is hosted by AT&T at a secured data center on dedicated servers. The data center is connected to the Port Authority network at our Network Operations Centers using two dedicated circuits. There are firewalls and other network equipment at each end of the circuits maintained separately by each party (AT&T and the Port Authority).

ii. Both the Port Authority and AT&T employ network intrusion detection and other security controls.

iii. Remote access to E-Mail is provided via a secure VPN system, through Outlook Web Access (OWA) access using Secure Socket Layers (SSL) with 128-bit encryption and via corporate mobile devices.

b. E-Mail Virus and Spam Protection and Content Scanning

i. The E-Mail servers utilize anti-virus software. All anti-virus software signature files are automatically updated regularly. This software scans E-Mails and removes detected viruses entering and leaving the E-Mail environment.

ii. The Port Authority uses additional anti-virus protection and anti-spam protection from a third party service provider which utilizes several industry-leading anti-virus engines, as well as proprietary software to identify and remove viruses from E-Mails and to quarantine E-Mails suspected of being spam.

iii. E-Mail Quarantined Reports are provided to each user. The user can access a secure web site to safely access these quarantined E-Mails in order to delete or release as appropriate. E-Mail is quarantined for 14 days prior to automatic deletion.

iv. Content filtering is used to identify potential spam E-Mail and when required, for handling certain forms of E-Mail related issues, e.g., E-Mail attacks, etc.

v. Following industry best practices to mitigate risk, certain attachments in E-Mails are blocked.

8. Desktop Patch Management

i. The Agency patching philosophy includes every security patch that can be applied to the Windows Operating System and the Microsoft Office suite of products.
ii. On the second Tuesday of every month, Microsoft releases hot fixes/patches/security bulletins for private and publicly reported vulnerabilities identified in their operating system and office suite of products. The monthly patches are pushed to the primary patch management distribution server within the Agency. TSD reviews all patches with a severity rating of Critical or Important. In addition, TSD performs lab testing to ensure no adverse effect is experienced during the deployment of the security updates.
iii. Once lab testing has been successfully completed, the monthly deployment is executed in three stages:
    1. Pre-Pilot Deployment
    2. Pilot Deployment
    3. Agency Deployment
iv. A feature of our patch management system is the “mandatory baseline” that will deploy the patches to any computer that is recently added to PAWANET as new or re-imaged.

9. Server Patch Management

i. The Agency patching philosophy includes every security patch that can be applied to the Windows Operating products.
ii. On the second Tuesday of every month, Microsoft releases hot fixes/patches/security bulletins for private and publicly reported vulnerabilities identified in their operating system and office suite of products. The monthly patches are pushed to the primary patch management distribution server within the Agency. TSD reviews all patches with a severity rating of Critical or Important.
iii. All servers deployed within the Agency must be patched on a regular basis using the management framework established in our Standard Operating Procedure For Applying Desktop and Server Patches Within the Port Authority Enterprise document, which from time-to-time will be updated to reflect current patching procedures.
iv. All servers deployed within the Agency must have the appropriate patches tested prior to deployment into a production setting.
v. All servers patched within the Agency must have a ‘Change Control’ log entry documented and a ‘Maintenance Window’ identified.

10. Content Management

i. The Port Authority’s Content Systems (a.k.a., PACS) provides a highly scalable and secure platform for the storage and management of electronic documents, collaboration and automated workflow for varying business applications across

the Agency. The PACS platform consists of a series of best-in-breed applications that when combined manage documents, drawings, forms, photos, video and architectural models. The PACS provides the following services:

1. Storage and Archival
2. Permissions and Privileges
3. Client-less Viewing
4. Full Text Search
5. Forms and Data Collection
6. Digital Visual Rights Management
7. Workflow
8. Collaboration Services

ii. PACS is the primary method for sharing in-process and milestone documents with partners, consultants, contractors and other Agencies via external Internet-based access. The PACS repositories are layered with the protections best suited for the information managed, as follows:

1. Proposed users of the system must request access via a uniform process that requires both business unit and TSD approval and coordination.
2. Access is linked directly to the PAWANET based authentication protocols and policies.
3. Users external to the Authority must sign NDA's and operate within contract requirements pledging compliance with PANYNJ information handling procedures.
4. Both external and internal users may undergo background checks prior to being granted access to PACS repositories or content. *Please refer to the Agency's Information Security Handbook (http://eNet.panynj.gov/home/pdf/Corporate-Information-Security-Handbook.pdf).*
5. User based activity, for both common users and administrators, are captured in a detailed and unalterable Audit Trail that is accessible by authorized individuals via the standard user interface.
6. PACS repositories may be physically isolated from one another due to specific business needs or enhanced security requirements.
7. Separate internal and external authentication schemes are maintained and monitored for security and reliability providing additional controls for external clients.
8. All PACS servers are located in PANYNJ Data Centers that provide for fault tolerance, physical and environment security systems.

9. Utilizes Agency's standard virus protection to ensure that documents passed into the PACS and maintained in the repository are scanned at multiple points in the information life-cycle.
10. Internet-based access is controlled by additional layers of authentication managed via reverse proxy and remote access protocols (further described within these Guidelines).
11. Multiple firewalls allow for specific access across approved ports between each of the application servers and in-line authentication devices (further described within these Guidelines).
12. Application servers are physically separate from Database servers and have no direct communication to external connections.
13. Dual form factor authentication is utilized for external access.
14. Database, Document Store and Index encryption technologies are utilized for ports of the PACS.
15. Intruder detection systems are employed to detect unauthorized access internally or externally to PACS application servers.
16. Server hardening and testing protocols are reviewed for each new piece of hardware introduced into the environment and periodically throughout its life.
17. PACS operates within the Agency's Change Management and Patch Management programs and policies.

Parking Access and Revenue Control System—Design, Installation & Maintenance

Attachment N
Example Escrow Agreement

Attachment N: Example Escrow Agreement

This agreement ("Agreement") made and entered into by and among [escrow Agent full name], having a principal place of business at [Agent address ("Agent")], [Contractor full name], having a principal place of business at [Contractor address ("Contractor")], and the Port Authority of New York and New Jersey, having a principal place of business at [Authority address ("Authority or Licensee")]. [Contractor full name] is referred to, in this agreement, as "Contractor".

This Agreement is made pursuant to Contract X calling for the establishment of an Escrow Agreement between the Authority and the Contractor.

Whereas Contractor and Licensee have entered into a Software License and Agreement dated _____ ("License Agreement") pursuant to which Contractor has agreed to grant Licensee a license to use certain computer software programs and related documentation upon specified terms and conditions; and

Whereas, pursuant to the Software License and Agreement, the programs will be installed and accepted by Licensee upon issuance of the Certificate of Final Completion under Contract X; and

Whereas, pursuant to the License Agreement, Contractor acknowledges that Licensee's ability to adequately utilize programs received under the License Agreement would be seriously jeopardized in the event of Contractor's failure to maintain and support such programs; and

Whereas, Contractor has agreed to establish and maintain in escrow the source code and documentation relating to the programs.

Now, therefore, in consideration of the premises and the mutual covenants contained herein, the parties agree as follows:

A. Deposit In Escrow

1. Initial Deposit. Within ten (10) days after execution of this Agreement, Contractor shall deposit into escrow with the Agent, Licensed Programs and Materials as defined in the Software License and Agreement, for the then-current version of the Software. Source code programs shall be submitted both on industry standard media and in printed, human-readable form, the same being collectively referred to hereinafter as the "Source Material." Contractor shall identify each item being delivered and certify the completeness and accuracy of the Source Material in an accompanying letter to the designated Agent and will transmit a copy to Licensee. Within five (5) days after receipt of the Source Material, Agent shall notify Licensee of such receipt. (Exhibit A hereof describes the procedure for initial and subsequent escrow deposits and Exhibits B and C hereof set forth a description of the Source Material to be deposited by Contractor.)

2. Revision Deposits. Contractor shall deliver revisions of the Source Material to Agent as and when corresponding revisions of the object code for the programs either become publicly available or available to Licensee under the License Agreement. At such time as any revisions to the Source Material are deposited, Agent shall give written notice of such deposits to Licensee which shall include Contractor's certification of their completeness and accuracy.

3. Deposit Procedure. The procedure defined in Table A-1 of Exhibit A is to be completed for the initial deposit and each annual or other major deposit. Its completion and the readiness of material to be put in escrow shall be signified in writing by the Licensee and the Contractor prior to turning the material over to the escrow Agent for storage. Table A-2 of Exhibit A defines the procedure and requirements for verification of the escrow deposit by the Licensee and the Contractor.

The initial and subsequent deposits are comprehensive replacements of all changed materials. If Licensee and Contractor agree, intermediate updates resulting from system changes may be accomplished by adding changed documents and program changes (including "makefiles" instructions, etc. required to install the changes) to the escrow package. If Licensee and Contractor are unable to agree to this abbreviated deposit procedure for a given update, the procedure described in Exhibit A shall be followed.

4. Warranties. The Contractor represents and warrants that the machine readable source code among the escrow materials shall be accurate, current, fully commented, complete, and compilable copies of all licensed software with release and version numbers specified and software required to compile, edit, and execute the programs; all of which are free of so- called computer viruses, Trojan Horses or other devices that would damage or render inoperable or unreadable any of the escrowed materials. Contractor further warranties that all documentation and other material necessary to maintain and modify each software component is included in the escrow package.

5. Storage Conditions. Agent shall hold the Source Material in a climate-controlled facility and shall release the same upon the terms and conditions hereinafter provided. Agent shall identify, in a written report, the escrow location to Licensee and Contractor.

B. Release From Escrow

1. Delivery by Agent to Licensee. Agent agrees that the Source Material shall be held by it for release and delivery to Licensee, under the terms and conditions hereinafter set forth, but only in the event that:

a. Contractor notifies Agent in writing to effect delivery to Licensee at a specific address, the notification being accompanied by a certified or cashier's check plus any amounts outstanding to Agent under this Agreement; or

b. Agent has received from Licensee all of the following:

(i) written notification that Contractor has failed to support the programs as required by the license agreement or has otherwise defaulted under the license agreement or any other agreement wherein Contractor has agreed to maintain the programs for Licensee ("Contractor default") (Contractor default shall also include Contractor's cessation of business operations or transfer of all or substantially all of its assets or obligations set forth in the license agreement to a third party which has not assumed all of Contractor's obligations under the license agreement and any companion maintenance agreement or Contractor has decided to stop supporting the programs);

(ii) evidence satisfactory to Agent that Licensee has previously notified Contractor of such Contractor default in writing and that more than sixty (60) days have elapsed since said notice with no cure by Contractor;

(iii) written demand that the material be released and delivered to Licensee;

(iv) a written undertaking from the Licensee that the material being supplied to the Licensee will be used only as permitted under the terms of the license agreement;

(v) specific instructions from the Licensee for this delivery; and

(vi) a certified or cashier's check payable to Agent in an amount equal $_____ plus any amounts outstanding to Agent under this agreement.

c. In the event that the provisions of paragraph b above are met, Agent shall, within five (5) days of receipt of all of the items specified above, send by certified mail, a copy of all such documents received by it to Contractor. Contractor shall have ten (10) days from the date Agent shall have sent the documents to Contractor to send to Agent written notice of its objection to the release of a copy of the Source Material. If, within ten (10) days after mailing the items specified in paragraph b above to Contractor, Agent has not received written notice of Contractor's objection to the release of the Source Material and its request for arbitration, then Agent shall release the Source Material and its request for arbitration to the Licensee in accord with the instructions specified in paragraph b (v) above.

2. Delivery by Agent to Contractor. Agent shall release and deliver the Source Material to Contractor upon the occurrence of any of the following.

a. Mutual Termination. The presentation to Agent of a written notice of termination, executed by authorized representatives of Contractor and the Licensee, stating that this Agreement has been terminated by the mutual agreement of Contractor and the Licensee and directing Agent to release and deliver the Source Material together with title thereto to Contractor by a specified method within ten (10) days of a specified date; or

b. Non-Payment. Upon non-payment of any fees or charges invoiced by Agent, Agent shall give notice of non-payment of any fee due and payable hereunder to both the Licensee and Contractor and, in such event, both the Licensee and Contractor shall have the right to pay the unpaid fee within thirty (30) days from the date of receipt of notice from Agent and upon timely payment of the unpaid fee by either the Licensee or Contractor, this Agreement shall continue in force and effect.

C. Ownership Of Source Material

1. Tangible Media. The tangible medium comprising the Source Material, but not the source code nor documentation and other information embodied in such tangible medium, shall belong to Agent at all times until the Source Material is returned to Contractor or turned over to the Licensee.

2. Intellectual Property. Agent, Contractor and Licensee recognize and acknowledge that ownership of the source code itself and any documentation (together with all copyrights, patent, trade secret, trademark and any other proprietary rights therein) shall remain with Contractor at all times. Agent shall have license to possess material deposited with it and Licensee when given possession shall possess license for use solely in compliance with this Agreement.

3. Confidentiality. The Contractor and Agent acknowledge that information stored and maintained under this Agreement, including those materials listed in Exhibits B and C to this agreement, is "Confidential and Proprietary Information" and they agree that they will not, during or after the term of this and successor agreements permit the duplication, use, or disclosure of any Confidential and Proprietary Information to any person or entity (other than their own employees, Agents, or representatives who must have such information) unless such duplication, use, or disclosure is specifically authorized by both the Authority and the Contractor.

D. Fees, Term, Renewal, And Termination

1. Agent Compensation. Agent shall be entitled to compensation described in Exhibit E for performance of its duties hereunder, to be borne by Licensee.

Agent's fee shall be paid by the Contractor until final acceptance as defined in Contract X and the Authority shall pay the fee subsequent thereto.

2. Term of Agreement. The initial term of this agreement shall extend until twenty years following completion of the applicable contract calling for the establishment of escrow material with Agent.

3. Renewal of Agreement. This agreement shall be automatically renewed for successive one (1) year terms unless otherwise terminated.

4. Termination of Agreement. This Agreement shall terminate upon (i) mutual termination as provided herein, or (ii) non- payment as provided herein, or (iii)

termination of the license agreement, or (iv) bankruptcy, receivership, or failure to fulfill responsibilities under this agreement as determined by the [customer nickname].

E. Source Material Accuracy

Agent shall have no responsibility with respect to the accuracy or completeness of the Source Material or any revisions thereto.

F. Bankruptcy

Contractor and Licensee acknowledge that this Agreement is an "agreement supplementary to" the License Agreement as provided in Section 365(n) of Title 11, United States Code (the "Bankruptcy Code"). Contractor acknowledges that if Contractor as a debtor in possession or a trustee in Bankruptcy in a case under the Bankruptcy Code rejects the License Agreement or this Agreement, Licensee may elect to retain its rights under the license and this Agreement as provided in Section 365(n) of the Bankruptcy Code. Upon written request of Licensee to Contractor or the Bankruptcy Trustee, Contractor or such Bankruptcy Trustee shall not interfere with the rights of Licensee as provided in the License Agreement and this Agreement, including the right to obtain the Source Material from Agent.

G. Liability

Except for actual fraud, gross negligence or intentional misconduct, Agent shall not be liable to Contractor or to any party claiming beneficiary status under this Agreement for any act, or failure to act, by Agent in connection with this Agreement. Any liability of Agent regardless of the cause shall be limited to the actual cost of new blank magnetic media or documentation of the same type and quality of any lost or destroyed source code copy. Agent will not be liable for special, indirect, incidental or consequential damages hereunder.

H. Indemnity

Contractor, Licensee, and any party claiming beneficiary status under this Agreement hereby agree to indemnity and hold harmless the Agent and each of its directors, officers, and stockholders, absolutely and forever, and from and against any and all claims, actions, damages, suits, liabilities, obligations, costs, fees, charges, and any other expenses whatsoever, including reasonable legal fees, that may be asserted against Agent or any of its directors, officers, or stockholders with respect to the performance of its duties under this Agreement, except as otherwise provided above.

I. Disputes And Interpleader

In the event of any dispute between Contractor and Licensee or any third party claiming beneficiary status under this Agreement, Agent may submit this matter to any court of competent jurisdiction in an interpleader or similar action. Any and all reasonable costs incurred by Agent in connection therewith shall be borne by the third

party seeking a copy of the Source Material. Without limiting the generality of the foregoing, if Agent shall be uncertain as to its duties or rights hereunder or shall receive any notice, advice, schedule, report, certificate, direction or other document from any person or entity with respect to the Source Material, that, in the opinion of the management of Agent is in conflict with any of the provisions of this Agreement, or shall be advised that a dispute has arisen with respect to the ownership or right of possession of the Source Material or any part thereof, Agent shall be entitled, without liability to anyone, to refrain from taking any action other than to exercise best efforts to keep safely the Source Material until Agent shall be directed otherwise in writing by an order, decree, or judgment of a court of competent jurisdiction that is then finally affirmed on appeal or that by the lapse of time or otherwise is no longer subject to appeal; but Agent shall be under no duty to institute or defend any such proceeding.

J. Governing Law

This agreement shall be construed and enforced in accord with the laws of the State of New York.

K. Verification

Upon receipt of a written request from Licensee or the Contractor, Agent is hereby authorized to inspect the Source Material to verify its relevance, completeness, currency, accuracy, and functionality. Upon request from Licensee or Contractor, Agent will issue a copy of the written technical verification report to Contractor.

Contractor hereby agrees to cooperate with Agent by providing its facilities, computer systems, and technical and support personnel for technical verification whenever necessary. If requested by Licensee, Contractor agrees to permit one employee of Licensee to be present at Contractor's facility during verification of Source Material.

The fee for this verification is specified in Exhibit E. It shall be paid by the requester.

L. Notices

All notices and other communications hereunder or in connection herewith shall be deemed to have been given if delivered personally or sent by registered or certified mail in writing, return receipt requested and first class postage prepaid.

A. If to Contractor: (insert name and full address)
B. If to Licensee: (insert name and full address)
C. If to Escrow Agent: (insert name and full address)

M. Binding Nature And Assignment

This Agreement shall be binding on the parties hereto and their respective successors and assigns, but no party may, or shall have the power to, assign this Agreement without the prior written consent, which shall not be unreasonably withheld, of the other parties. Contractor, however, shall have the right, without consent of any other party, to assign to a successor entity that portion of Contractor's business which is the subject of this Agreement.

N. Entire Agreement

This Agreement including any Exhibits or documents referred to in this Agreement, each of which is incorporated herein, constitutes the entire and exclusive statement of the agreement between and among the parties with respect to its subject matter and there are no oral or written representations, understandings or agreements relating to this Agreement which are not fully expressed herein.

O. Miscellaneous

1. Section Headings. The Section headings used in this Agreement are for reference and convenience only and shall not enter into the interpretation hereof.

2. Separability. If any provision of this Agreement is declared or found to be illegal, unenforceable or void, then obligations arising under such provision shall be null and void and each provision not so affected shall be enforced to the full extent permitted by law.

3. Waivers and Discharges. No delay or omission by any party hereto to exercise any right or power hereunder shall impair such right or power or be construed to be a waiver thereof. No change, waiver or discharge hereof shall be valid unless in writing and signed by an authorized representative of the party against which such change, waiver or discharge is sought to be enforced.

4. Responsibilities, Liabilities, Obligations upon Termination. Termination or expiration of this Agreement for any reason shall not release any party from any liabilities or obligations set forth in this Agreement which (i) the parties have expressly agreed shall survive any such termination or expiration, or (ii) remain to be performed or by their nature would be intended to be applicable following any such termination or expiration.

5. Personal Liability of Individuals. No commissioner, Agent, officer, or employee of any of the parties shall be personally liable hereunder.

6. Restrictions on Licensee's use of Source Material. During any period of time in which the Source Material is in the possession of the Licensee, it is agreed that the Source Material shall be used only by the Licensee at the locations set forth in the license agreement and shall not be duplicated, sold, or licensed to others or marketed in any manner. In addition, during this time Contractor shall have unrestricted use and title

to the Source Material and any associated object code for its own internal use or for marketing to third parties.

1. EXHIBIT A - INITIAL, MAJOR UPDATE, AND ANNUAL ESCROW DEPOSIT PROCEDURES

Table A-1 Primary Deposit Procedure

	PROCEDURE	RESPONSIBLE
1	Contractor prepares escrow material, defined in Exhibit B, below, representing the current application as installed, accepted, and in production use.	Contractor
2	Authority staff witness compilation and verification, conducted by Contractor under the conditions defined in Table A-2, below, to ensure that software matches current production modules, verifies that all software needed to convert the source programs to executable modules are licensed to the Authority, installed on Authority computers, and fully operational.	Authority
3	Representatives of Authority and the Contractor inspect the escrow package and verify that it represents the current production package.	Authority, Contractor
4	Representatives witness package sealing and transmit to the escrow Agent.	Authority, Contractor
5	Each time there is a revision and/or upgrade of the Source Material of the Production System, or if not changed or modified at least once each year, the three parties open the package, update its contents to reflect the current production system and document the activity to reflect the current installed version.	Authority, Contractor, Agent

Table A-2 Deposit Verification Procedure

	PROCEDURE	RESPONSIBLE
1	Contractor prepares escrow material and notifies the Authority that the complete deposit, computer platforms for verification, and software tools for verification are ready.	Contractor
2	Authority and Contractor staff meet at an Authority or Contractor site agreed to and Contractor conducts compilation and verification, to the Authority's satisfaction, of all software and firmware to be put in escrow to ensure that the Source Material in the deposit matches current production modules (through the use of tools or utilities that use an industry standard CRC (cyclic redundancy check) checksum or other process acceptable to the Authority that separately authenticates all files and modules, absent file names, dates, times, and other header and identification information that might prevent comparison, and lists all file names with their validating information). The process must include the compilation/assembly and linking of all modules required on appropriately configured platforms.	Authority, Contractor
3	Contractor and Authority staff conduct such operations as are needed to verify the completeness and functionality of the tools (compilers, assemblers, linkers, editors, etc.) complete with documentation; procedures and makefiles; operating system, communications, and environment software; and any other materials.	Contractor, Authority
4	Contractor and Authority staff examine all documents included to ensure that they are complete and correctly reflect the production system.	Contractor, Authority
5	Authority and Contractor staff examine all software literature and licenses and verify that all software needed to convert the source programs to executable modules are properly licensed to the Contractor, installed on	Contractor, Authority

	Authority computers, and fully operational.	

2. EXHIBIT B - MATERIAL TO BE DEPOSITED BY CONTRACTOR

- Human readable Source Code for all Contractor Proprietary and Custom Software in an industry standard electronic medium (e.g. diskette or CD-ROM).
- Human readable and printed program, system, user documentation either in printed form or in an industry standard electronic medium (e.g. diskette or CD-ROM)
- Tools (compilers, assemblers, linkers, etc.) with documentation.
- Procedures and makefiles.
- Other documentation which includes: a listing of all program and module inputs and their sources, outputs and their destinations, and other relevant program and module documentation.
- Operating system, communications, and environment software.

NOTE: Where actual copies of licensed software are accepted by the Authority as being prohibited under the provisions of the license, the Contractor shall include complete identification of each software product including manufacturer/publisher, version, release, and all information required for acquisition and use.

3. EXHIBIT C - MATERIAL TO BE DEPOSITED BY SUBCONTRACTORS AND/OR SUPPLIERS RELATED TO SOFTWARE AND EQUIPMENT SUPPLIED BY THEM

- Human readable Source Code for all Sub-Contractor Proprietary and Custom Software (as defined in the License Agreement) in an industry standard electronic medium (e.g. diskette or CD-ROM).
- Human readable program, system, and user documentation either in printed form or in an industry standard electronic medium (e.g. diskette or CD-ROM).
- Tools (compilers, assemblers, linkers, etc.) with documentation.
- Procedures and makefiles.
- Other documentation listing program and module inputs and their sources, outputs and their destinations, and other relevant program and module documentation.
- Operating system, communications, and environment software.
- All other material as agreed to by Contractor and the Authority.

NOTE: Where actual copies of licensed software are accepted by the Authority as being prohibited under the provisions of the license, the Contractor shall include complete identification of each software product including manufacturer/publisher, version, release, and all information required for acquisition and use.

4. EXHIBIT D - MATERIAL TO BE DEPOSITED BY CONTRACTOR AND SUPPLIED TO ESCROW AGENT, CONTRACTOR AND THE AUTHORITY

A complete escrow inventory with release dates, release numbers, version numbers, etc.

5.

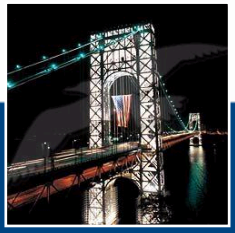
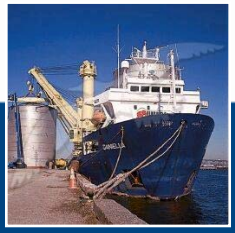
6. EXHIBIT E - FEES TO BE PAID

Initialization fee (one time only)	$ _____
Annual maintenance / storage fee (includes one deposit material update per year)	$ _____
Additional updates	$ _____
Due upon request for release of material	$ _____
Agent inspection at Licensee / Contractor request	$ _____
Additional work at Licensee / Contractor request	$ _____

After expiration of the initial term of this Agreement, this Agreement shall be automatically renewed for successive years unless otherwise terminated.

Parking Access and Revenue Control System—Design, Installation & Maintenance

Attachment O
Information Security Handbook

The Port Authority of New York & New Jersey

Information Security Handbook

October 15, 2008, corrected as of November 14, 2013

The Port Authority of New York and New Jersey

Information Security Handbook

Copyright © 2008, 2013 The Port Authority of New York and New Jersey

No copyright is claimed in the text of U.S. regulations or statutes quoted within.

TABLE OF CONTENTS

Page

INTRODUCTION 1

CHAPTER 1

PORT AUTHORITY INFORMATION SECURITY ORGANIZATIONAL STRUCTURE..... 2

CHAPTER 2

CATEGORIZATION OF INFORMATION 4

2.1 DEFINITIONS 4

2.2 GENERAL PROCESS FOR CATEGORIZATION 5

2.3 TRAINING AND INFORMATION REVIEW..... 6

2.4 REMOVAL OF CATEGORY DESIGNATION 7

CHAPTER 3

INFORMATION ACCESS..... 8

3.1 APPLICABILITY 8

3.2 GENERAL CRITERIA..... 8

3.3 INFORMATION ACCESS CONTROLS..... 9

3.4 ACCESS DISQUALIFICATION 11

3.5 NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENTS (NDAs)..... 11

3.6 UNAUTHORIZED DISCLOSURE OF INFORMATION 12

3.7 SECURITY CLEARANCE AND ACCESS PROHIBITIONS..... 12

3.8 BACKGROUND SCREENING 12

3.9 AUTHORIZED PERSONNEL CLEARANCE LIST..... 13

3.10 DEVELOPMENT OF CONFIDENTIAL INFORMATION
PRACTICES AND PROCEDURES (CIPP)..... 13

3.11 PROCUREMENT STRATEGIES 14

CHAPTER 4

MARKING, HANDLING, STORAGE, TRANSMITTAL AND
DESTRUCTION REQUIREMENTS 17

4.1 MARKING OF PROTECTED INFORMATION..... 17

4.2 HANDLING PROTECTED INFORMATION..... 19

4.3 TRANSMITTAL OF PROTECTED INFORMATION 19

4.4 STORAGE OF PROTECTED INFORMATION..... 22

4.5 DOCUMENT ACCOUNTABILITY LOG..... 22

4.6 REPRODUCTION 23

4.7 DESTRUCTION OF PROTECTED INFORMATION..... 23

4.8 INFROMATION TECHNOLOGY SYSTEMS
HANDLING OF ELECTRONIC INFORMATION /DATA ……24

4.9 TRANSMISSION/EXCHANGE OF ELECTRONIC INFORMATION ……..24

4.10 ELECTRONIC STORAGE ……25

4.11 USER ACCESS DEACTIVATION ……26

CHAPTER 5

AUDITING AND MONITORING 27

5.1 PURPOSE 27

5.2 AUDITS AND INVESTIGATIONS 27

5.3 SELF-ASSESSMENT 28

CHAPTER 6

POLICY VIOLATIONS AND CONSEQUENCES 29

6.1 RESPONSIBILITIES 29

6.2 VIOLATIONS, INFRACTIONS, OR BREACH OF INFORMATION SECURITY PROTOCOLS 29

6.3 VIOLATION REPORTING, INVESTIGATION AND FACT FINDING 29

6.4 DISCIPLINARY ACTION 29

CHAPTER 7

INFORMATION SECURITY EDUCATION AND AWARENESS TRAINING 31

7.1 PURPOSE 31

7.2 OVERVIEW 31

7.3 TRAINING PROGRAM ELEMENTS 31

APPENDICES OF HANDBOOK

A - PROTECTED INFORMATION

B – NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENTS

B-1: Non-Disclosure and Confidentiality Agreements with reference to Handbook

B-2: Non-Disclosure and Confidentiality Agreements without reference to Handbook

B-3: PA/PATH Employee Non-Disclosure and Confidentiality Agreement

C – BACKGROUND SCREENING CRITERIA

D – THE SECURE WORKER ACCESS CONSORTIUM (SWAC)

E – COVERSHEET FOR CONFIDENTIAL PRIVILEGED INFORMATION

F – TRANSMITTAL RECEIPT

G –GUIDELINES FOR THE STORAGE OF PROTECTED INFORMATION

H– GUIDELINES FOR THE DISPOSAL AND DESTRUCTION OF PROTECTED INFORMATION

I- AUDIT PROCEDURES

INTRODUCTION

This *Port Authority of N.Y. & N.J. Information Security Handbook* ("Handbook") establishes guidelines and uniform processes and procedures for the identification, handling, receipt, tracking, care, storage and destruction of Protected Information (as hereinafter defined) pursuant to The Port Authority of New York and New Jersey Information Security Policy (the "Policy"). This Handbook is intended to be the implementation guideline for that policy. It is also intended to complement the Port Authority Freedom of Information Code (Code), inasmuch as it further defines certain information that may be exempt from release under the Code. The guidelines contained in this Handbook are not intended to, in any way, be in derogation of the FOI Code adopted by the Board in March 2012. The Code continues to provide open, timely and uninhibited access to the Port Authority's (and its subsidiary corporations') public records and reflects the New York Freedom of Information Law ("FOIL") and New Jersey's Open Public Records Act ("OPRA"). . This Handbook prescribes requirements and other safeguards that are needed in order to prevent unauthorized disclosure of Protected Information and to control authorized disclosure and distribution of designated sensitive information, when it is released by The Port Authority of New York and New Jersey (the "Port Authority") either internally or externally. A major underlying principle, on which the Handbook is premised, is that there is a limited universe of sensitive information to which it applies. There is the expectation that prudent, informed and circumscribed judgments will be made by those staff members charged with the responsibility of identifying and properly designating sensitive information, as is provided for in this Handbook. In this regard, adherence to the Handbook's requirements will help ensure that the necessary care will be constantly and consistently undertaken in order to ensure that mis-designation, or "over marking", of information will be avoided. Another important principle of the Handbook is that access to properly designated sensitive information is premised on a strict "need to know" basis. It is the establishment of this "need to know" that is the essential prerequisite for being granted access privileges. It must be emphasized that possession of a federal security clearance or other access rights and/or privileges to sensitive information does not *per se* establish a "need to know" for purposes of obtaining access to discrete sensitive Port Authority information. This principle is equally applicable to the Port Authority and its internal staff as it is to third party individuals and entities, which are given access privileges to sensitive Port Authority information.

This Handbook will be amended and updated from time to time as may be appropriate. When appropriate, each Port Authority department, office and/or business unit, as well as contractors/consultants, should create a "Confidential Information Practices and Procedures" ("CIPP") document with additional guidelines for their respective businesses. This will assist staff, and third parties working with the Port Authority, in carrying out the requirements of this Handbook. A CIPP should augment, but may not deviate from, the requirements of this Handbook. The procedures, safeguards and requirements of this Handbook fully apply to all subsidiaries of the Port Authority that deal with, or create, Protected Information. Whenever the term Port Authority is referenced in this Handbook, it should be understood to include and/or cover its subsidiary entities.

<u>The Port Authority expressly reserves the right to reject any information designation and/or to remove/add any and all markings on information that is not consistent with this Handbook.</u>

CHAPTER 1 - PORT AUTHORITY INFORMATION SECURITY ORGANIZATIONAL STRUCTURE

The Port Authority organizational structure for information security is as follows:

Chief Security Officer (CSO) – is responsible for the implementation of Port Authority policy on security matters, both physical and informational, and for the coordination of security initiatives throughout the agency in order to assure consistency in practices, procedures and processes. In particular, the CSO works in close collaboration with the Director of Technology Services Department and the Corporate Information Security Officer with regard to their respective areas of security responsibilities. The CSO acts as the Port Authority's principal liaison on security related matters with governmental, public and private entities. The CSO works closely with the Law Department, Public Safety Department and the Office of Inspector General on security initiatives, on compliance with governmental requirements on security matters, and on issues relating to compliance with the Port Authority's security policy.

Corporate Information Security Officer (CISO) – the CISO reports directly to the CSO in order to assure agency wide consistency on policy implementation. The CISO is responsible for the management, oversight and guidance of the Policy. The CISO works in conjunction with all appropriate Port Authority departments and subsidiaries to: (i) formulate practices and procedures concerning information security management issues affecting the Port Authority, its operations and facilities; (ii) review, categorize and manage all Port Authority information consistent with the Port Authority's policy and procedures under its Freedom of Information Code; and (iii) establish procedures and handling requirements for Port Authority information based upon its sensitivity designation in order to ensure that the information is used solely for authorized purposes. The CISO will report to the Secretary who in turn reports to the Executive Director.

Departmental Information Security Officer (DISO) - each department head, and, where appropriate, office head, will designate a staff member to act as DISO in order to ensure compliance with the Policy. The DISO is responsible for management and oversight of information security issues for departmental operations and reports to the CISO on information security practices and procedures, or issues relating thereto. Additionally, the DISO may perform the Security Information Manager (SIM) functions, if a SIM has not been designated for a department, division, office, unit or project. Each DISO is also responsible for compiling an inventory of all Confidential Privileged Information and Confidential Information in their department's possession and/or providing updated listings to the CISO on a monthly basis, or on such other periodic basis as may be established by the CISO. Additionally, the DISO is responsible for approving the departmental Confidential Information Practices and Procedures ("CIPP") document and, before authorizing its use, for submitting the CIPP to the CISO for final approval and providing periodic reports to the CISO, as the CISO may require.

Security Information Manager (SIM) – Port Authority departments, offices or other business units, as well as contractors, vendors, and consultants, individuals and/or entities, where appropriate, who are involved with, or who could have exposure to, Confidential Information shall designate a SIM who is responsible for coordinating the implementation and daily oversight of the Policy for the particular Port Authority department, office, business unit, or third-party contractor, vendor, or other party. The SIM reports to the DISO and/or the Security Project Manager (SPM) for a project, where applicable. If a Port Authority department

determines that the SIM function may be carried out by the DISO, then the SIM designation may not be required, unless or until the DISO, in consultation with the CISO, determines otherwise. The functions of the SIM are further described throughout this Handbook.

Director of Technology Services Department– is the head of the Technology Services Department (TSD). The Director of TSD, or the Director's designee, works with the CSO and the CISO to coordinate the Policy efforts and to provide the Port Authority with the most current resources needed to comply with legislative and regulatory requirements, to adhere to industry standards and best business practices and procedures, and to identify and address technology issues that may affect the current and future policy. The Director of Technology Services Department is also responsible for providing technical support and training to assist staff and to meet information security management goals.

Office of Inspector General (OIG) – The OIG's responsibilities include: conducting criminal and administrative investigations of possible misconduct by Port Authority officers and employees, as well as third parties doing business with the Port Authority; reviewing agency internal controls and management practices for weaknesses that could allow losses from corruption, incompetence and/or bad decision making; making recommendations for cost effective improvements; serving as the confidential investigative arm for the Port Authority's Ethics Board; conducting educational awareness programs for all Port Authority employees pertaining to integrity and ethics; and, where appropriate, conducting background investigations of certain contractors proposing to do business with the Port Authority. The OIG's Security Inspection Division is responsible for conducting investigations, inspections, reviews, and audits pertaining to all Port Authority security programs in all departments. It should be noted that cases involving investigations are exempt from CISO approval.

Information Security Subcommittee (ISSC), chaired by the CISO, includes departmental representatives from line departments (who might also be functioning as a DISO), the Law and Public Safety Departments, the Office of Inspector General and the Director of Technology Services Department. The ISSC assesses the Policy needs and the effectiveness of the policy's implementation, as well as evaluating initiatives for its further development and refinement.

CHAPTER 2 - CATEGORIZATION OF INFORMATION

2.1 Definitions

For purposes of this Handbook the following definitions shall apply:

(a) "**Information**" means, collectively, all documents, data, reports, notes, studies, projections, records, manuals, graphs, electronic files, computer generated data or information, drawings, charts, tables, diagrams, photographs, and other media or renderings containing or otherwise incorporating information that may be provided or made accessible at any time, whether in writing, orally, visually, photographically, electronically or in any other form or medium, including, without limitation, any and all copies, duplicates or extracts of the foregoing.

(b) "**Protected Information**" means and includes collectively, Confidential Information, Confidential Privileged Information, Sensitive Security Information (SSI), Critical Infrastructure Information (CII) or Health Insurance Portability and Accountability Act (HIPPA) and Information that is labeled, marked or otherwise identified by or on behalf of the Port Authority so as to reasonably connote that such information is confidential, privileged, sensitive or proprietary in nature. The term Protected Information shall also include all work product that contains or is derived from any of the foregoing, whether in whole or in part, regardless of whether prepared by the Port Authority or a third-party, or when the Port Authority receives such information from others and agrees to treat such information as Protected.

(c) "**Confidential Privileged Information**" means and includes collectively Information that reveals security risks, threats, vulnerabilities, documentation that identifies specific physical security vulnerabilities or revealing specific security vulnerabilities details related to emergency response protocols, egress plans, flow paths, egress capacities, (diagrams, codes, standards) etc., which is not publicly available." and any and all Information, documents and materials entitled to protection as a public interest privilege under New York State law and as may be deemed to be afforded or entitled to the protection of any other privilege recognized under New York and/or New Jersey state laws or Federal laws.

(d) "**Confidential Information**" means and includes collectively, any and all Information, documents and materials entitled to protection as a public interest privilege under New York State law and as may be deemed to be afforded or entitled to the protection of any other privilege recognized under New York and/or New Jersey state laws or Federal laws. It also includes Information that contains sensitive financial, commercial or other proprietary business information concerning or relating to the Port Authority, its projects, operations or facilities that would be exempt from release under the Port Authority Freedom of Information Code. It also includes sensitive financial, commercial and other business information received from third parties under Non-Disclosure and Confidential Agreements.

(e) "**Health Insurance Portability and Accountability Act (HIPAA)"** Employees, associates or other contract personnel who have access to Protected Health Information (PHI) must refer to, and comply with, the Privacy Policies and Procedures to Protect Personal Health Information. Privacy regulations issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA" or "Privacy Laws") place restrictions on the Group Health Plans of the Port Authority and PATH (the "Plans") ability to use and disclose Protected Health Information ("PHI").

(f) "**Attorney Work Product"** Attorney work product and other privileged information should be protected and treated in accordance with the established rules of the legal profession and may carry the label "Privileged & Confidential" or "Attorney Work Product". Certain attorney work product information may also fall within the definitions of Confidential Privileged and/or Confidential Information as established by the Handbook, and as such, should be marked and treated in accordance with the Handbook and the Law Department CIPP.

(g) "**Critical Infrastructure Information**" (CII) has the meaning set forth in the Homeland Security Act of 2002, under the subtitle Critical Infrastructure Information Act of 2002 (6 U.S.C. §131-134), and any rules or regulations enacted pursuant thereto, including, without limitation, the Office of the Secretary, Department of Homeland Security Rules and Regulations, 6 C.F.R. Part 29 and any amendments thereto. CII may also be referred to as "Protected Critical Infrastructure Information" or "PCII," as provided for in the referenced rules and regulations and any amendments thereto.

(h) "**Sensitive Security Information**" (SSI) has the definition and requirements set forth in the Transportation Security Administrative Rules & Regulations, 49 CFR 1520, (49 U.S.C. §114) and in the Office of the Secretary of Transportation Rules & Regulations, 49 CFR 15, (49 U.S.C. §40119) and any amendments thereto.

(i) "**Non-Disclosure and Confidentiality Agreement**" (NDA) refers to the Agreements attached hereto as Appendix "B" (which include Appendices B-1 through B-3). When approved by the Law Department, other forms of a NDA may be used for special situations or specific projects, however, a general NDA may be used in retaining consultants and contractors where the retainer involves work on various projects.

(j) "**Non-Disclosure Instructions**" (NDI) refers to the instructions attached hereto as Appendix "C." A NDI is used when represented staff are given or have responsibilities, which involve working on sensitive and/or security related matters, and/or when such staff is being given access to Confidential Information. The NDI is given to each individual before starting such work or on being given such access. The CISO, in consultation with the Law Department, may allow the use of NDI's in other circumstances, as may be appropriate.

2.2 General Process for Categorization

As defined hereinabove, the term Protected Information includes all Port Authority Information protected pursuant to this Handbook or as governed by statutory regulations. Any sensitive Information not specifically deemed Confidential Privileged Information should be categorized as Confidential Information. In addition, certain other types of Protected Information, such as HIPAA, SSI and CII, are treated separately and distinctly because they are governed by specific federal designations and must be marked and handled in accordance with federal regulations or requirements. The requirements in this Handbook apply to all Protected Information, unless otherwise specified. Where a different or additional requirement applies to a specific sub-category of Protected Information, it will be noted.

Each DISO, in consultation with the CISO, shall create a list of examples of Confidential and Confidential Privileged Information to be used as a guide by the departmental staff. This list may be included in the department's CIPP. Any employee, consultant, third-party contractor or other agency personnel may nominate Information for categorization in either of the two categories. The DISO, SIM, supervisors, managers or the CISO, as may be appropriate, should take the action needed to process the Protected Information under their control and to review it as soon as possible. It is important to understand that not every piece of material currently held should be reviewed. The review should only be of Information that is considered potential Protected Information. If management, employees, consultants, third-party contractors, or other agency personnel determine that Information under review contains Protected Information, the Protected Information should be designated with the appropriate categorization.

In order to categorize Information as Confidential Privileged Information or Confidential Information the following steps must take place:

1. Inform the DISO or SIM, where applicable, and the unit supervisor of the group/entity proposing the categorization.
2. Obtain DISO concurrence and approval.
3. Obtain CISO approval (except in the case of the PA OIG).
4. If approved, mark and label the information, and, if appropriate, apply a cover sheet (See Appendix F).

If Information has been nominated for Confidential or Confidential Privileged categorization, a final decision on the nomination shall be made within one week of its submission. During the time period between the submission and a determination regarding the categorization, the nominated Information should not be reviewed, released or distributed to any individuals, other than those individuals who possess a need to know and are currently familiar with the Information, or were previously provided access to other Confidential or Confidential Privileged Information for the same project or task.

2.3 Training and Information Review

Port Authority managers, including, but not limited to, the DISO, SPM and the SIM will complete training. This enables them to conduct a continuing review of Protected Information under their control in order to identify and categorize it as Confidential or Confidential Privileged Information. Employees, consultants, third-party contractors or other agency personnel must participate in and complete the Policy training, which enables them to continue the process of review, identification, and categorization of Protected Information.

Each Department Director will determine which staff members in the respective department require Policy training and will do so on an ongoing basis. When access to Protected Information is given to third parties, a training requirement may also be a condition for granting access privileges.

2.4 Removal of Category Designation

At some point, Protected Information may no longer be considered Confidential or Confidential Privileged, and should therefore have its designation removed or eliminated. This may occur as a result of any number of circumstances, including changes within the Policy, the changing nature of information security, a better understanding of particular material, and/or changes in public policy or law, among others. In order to determine whether category designations should be removed from particular materials, the CISO may establish criteria for the periodic review of all sensitive material. In any case, the category designation of any particular Protected Information may not be removed without the approval of the CISO. A record of any removal of categorization for particular information must be kept by the DISO, with a copy provided to the CISO.

CHAPTER 3 – INFORMATION ACCESS

3.1 Applicability

Each employee, consultant, third-party contractor, tenant, individual and/or entity requiring, or requesting, access to Port Authority Protected Information must adhere to the requirements set forth in this Handbook.[1] Protected Information is intended for official business use only. Failure to abide by the procedures set forth in the Handbook can lead to a denial of access privileges to Protected Information and/or other contractual, civil, administrative or criminal action.

All employees, consultants, third-party contractors, individuals and/or entities given access privileges to Protected Information are responsible for overseeing the safeguarding and protection of Protected Information in their possession or under their control as per this Handbook's requirements. Questions concerning the safeguarding, protection, release, and/or access to Protected Information should immediately be brought to the attention of the CISO, DISO, SPM, or SIM, as may be appropriate, in the particular circumstance.

3.2 General Criteria

In order for access to certain Protected Information to be considered for approval, all individuals including PA staff, must meet and complete the following criteria, unless otherwise required under federal or state regulations:

- Be a citizen of the United States of America, or be an alien who has been lawfully admitted for permanent residency or employment (indicated by immigration status), as evidenced by Immigration and Naturalization Service documentation, or be a national of the United States as defined by the Immigration and Nationality Act. This requirement may be waived by the CISO with the concurrence of the OIG and/or the CSO where and when circumstances so require.
- Obtain sponsorship for a request to be given access to Protected Information through the individual's assigned chief, director, manager, or supervisor. The written request must include justification for access, level of access required, and indicate the duration for which access privileges are required. (OIG is exempt from this)
- Forward the request through the individual's supervisory chain to the CISO, "(except in the case of the PA OIG) , via the appropriate DISO, SPM, or SIM, requesting that a specific background check be undertaken, where appropriate and/or required.
- Background check required to access CP information and/or accessing a PA Facility that requires background screening."

- Complete the Port Authority Information Security Education and Awareness Training.

---

[1] The CSO and/or the OIG in consultation with the Law Department may modify and/or waive the condition of complying with the requirements of the Handbook where such compliance is impractical, such as in the case of a governmental entity having its own information security procedures and/or protocols governing the handling and protection of sensitive information. In addition, certain sensitive information is required to be submitted to other governmental entities under applicable laws, rules or regulations, or the Port Authority may elect to submit Confidential Information to a governmental entity, such as in the case of the CII process, wherein it may elect to submit Confidential Information to the Department of Homeland Security in order to secure the protection of the CII regulatory scheme.

- Execute a Port Authority NDA (See Appendix B), or an Acknowledgement of an existing executed NDA, and, if the individual is Port Authority represented staff, have been provided with the NDI. Consultants or third party need's to designate a Security Information Manager (SIM)
- Be granted final approval of the security clearance level, in writing, by the CISO who verifies that all requirements have been met.

The individual's name must be entered on the appropriate department, or Port Authority Authorized Personnel Clearance List for access to Confidential and/or Confidential Privileged Information. See Sec. 3.9 for more information regarding this List (Note: If an individual's name does not appear on the appropriate Authorized Personnel Clearance List, access must be denied).

Individuals who meet and complete the criteria listed above are neither guaranteed, nor automatically granted, access to Protected Information, since access is conditioned on need to know criteria. The OIG may access, without approval of the CISO, DISO, SPM or SIM, all Protected Information when it is needed in connection with an OIG investigation, audit or inspection work, or any other Port Authority related work, subject to the handling requirements set forth in this Handbook.

3.3 Information Access Controls

Access to all Protected Information falling within any of the Port Authority Information categories shall be undertaken in a manner that complies with and maintains all applicable state, federal and common law protections. Access to particular Information must be conditioned upon a strict need to know basis with regard to the particular, discrete Information, regardless of any federal security clearance, or other Port Authority or other organizational information access authorization. An individual's need to know is not established simply by reason of the individual possessing a recognized federal security clearance, including one that allows for access to a higher level of classified information than is otherwise required for the discrete Port Authority Information to which access is sought. All requests for access to SSI by anyone who does not possess the requisite "need to know" under SSI regulations must be reported to the Transportation Security Administration ("TSA") or, if applicable, the United States Coast Guard ("USCG") and, in certain instances, the Department of Transportation ("DOT").

(a) Protected Information

Access to Protected Information shall be on a need to know basis only, as determined by the DISO. In certain limited instance's access, privileges may be conditioned on the satisfactory completion of a background investigation(s). The background investigation, if warranted, should utilize the least stringent criminal history access disqualification criteria that is appropriate for granting access to the particular information for both Port Authority and non-Port Authority employees. Where a background investigation is a condition to granting access, a DISO may determine that periodic updates of such investigations are required as a condition to maintaining continued access privileges. Access by third parties to certain Protected Information, such as Confidential Privileged, and/or Confidential Information, requires that the parties execute a NDA or an Acknowledgment of an existing NDA if the CISO or OIG determines that a NDA and/or Acknowledgment is required.

(i) Confidential Information

Access to Confidential Information shall be on a need to know basis only, as determined by the DISO. In certain instances, access privileges may be conditioned on the satisfactory completion of a background investigation(s). The background investigation should utilize the least stringent criminal history access disqualification criteria that is appropriate for granting access to the particular information for both Port Authority and non-Port Authority employees. Where a background investigation is a condition to granting access, a DISO may determine that periodic updates of such investigations are required as a condition to maintaining continued access privileges. Access by third parties to Confidential Information may require that the parties execute a NDA or an Acknowledgment of an existing NDA if the CISO or OIG determines that a NDA and/or Acknowledgment is required.

(ii) Confidential Privileged Information

Individuals requiring access to Confidential Privileged Information must have a need to know consistent with the creation and preservation of the privilege attaching to the particular Information. An individual will be given access privileges to the Confidential Privileged information only to the extent that it is necessary and/or is required by the individual in order to fulfill and/or carry out his/her duties, obligations and responsibilities to the Port Authority. Access to Confidential Privileged information is subject to the satisfactory completion of a background investigation for non-Port Authority individuals and to continuing periodic checks. A list of disqualifying crimes for the different levels of background screening is attached as Appendix "D." A more stringent background investigation may be required of the individual for access to certain Confidential Privileged Information if determined by the DISO. All access to such Information must be granted and received in a manner that does not compromise or abrogate the particular privilege attaching to the Information.

Confidential Privileged Information may not be disclosed to any individual without appropriate prior approvals. Approval for disclosure of Confidential Privileged Information to third parties must be obtained from the DISO. A Port Authority employee or other individual may not waive any privilege attaching to Port Authority Information without the Port Authority's express permission as granted by the CISO, unless the Information to which the Port Authority asserts a privilege is personal to a particular employee or individual and the privilege is directly derived by reason of that circumstance. Access by third parties to Confidential Privileged Information will be conditioned on the parties' execution of a NDA or an Acknowledgment of an existing executed NDA, as may be appropriate and determined by the CISO. In the case of certain represented employees/individuals, and in some cases NDIs may be utilized in lieu of NDAs upon the approval of the CISO.

3.4 Access Disqualification

Any employee, consultant, third-party contractor, or other individual and/or entity, who has been granted access to Protected Information, may be temporarily denied access while an investigation is conducted regarding any report to the CISO, OIG and the DISO that such individual misused, mishandled, or lost Protected Information, or disclosed, disseminated, or released Protected Information to an unauthorized individual or entity. Further, access to Protected Information can be denied when improper or incomplete verification checks of employees, entities, or individuals are discovered. In addition, if an individuals' SWAC has expired, or access level has changed that individual may no longer have access to Protected Information.

Where it is determined that an individual has misused, mishandled or otherwise improperly disclosed, released or disseminated Protected Information without authorization, that individual may be subject to disqualification of access privileges and may also be subject to sanctions, including formal disciplinary actions where the individual is a PA employee, with possible penalties up to and including termination of employment. The foregoing action shall be documented and provided to the individual's employer, SPM, DISO, or departmental manager, OIG, and the CISO, as may be appropriate. In the case of third parties, remedial action may include, but is not limited to, imposition of a monitor to oversee compliance with information security and general security requirements, or possible disqualification, and/or termination of present and/or future business relationships. Individuals and entities may also be subject to criminal or civil legal action, as may be appropriate. Additionally, see Chapter 6 regarding the possible consequences of violations of this Policy.

3.5 Non-Disclosure and Confidentiality Agreements (NDAs)

Employees, consultants, third-party contractors, tenants, or other individual or entities, including governmental agencies where appropriate, will be required to sign NDAs or an Acknowledgment of an existing NDA, or be subject to an NDI, as a condition of being granted access to Confidential Privileged Information and, where appropriate, Confidential Information. Employees, consultants, third-party contractors, or other agency personnel who refuse to sign a NDA, in situations where it is required, will be denied access to Confidential and/or Confidential Privileged Information, except in the case of certain Port Authority employees and third parties where a NDI may be utilized in instructing and advising the Port Authority employee and/or third party of the obligations and the requirements for handling Confidential Information. In certain circumstances, a Memorandum of Understanding or Memorandum of Agreement containing approved non-disclosure and confidentiality requirements may be utilized, in which cases approvals are required from the CISO and the General Counsel, or their respective designees. The DISO is responsible for determining whether a NDA/NDI is required as a condition to being granted access privileges to certain Protected Information, other than Confidential Privileged Information. If an individual refuses to execute an individual Acknowledgment, PA Employee NDA or to receive the NDI, if it is deem required by the DISO, CISO or OIG, access to the certain Protected Information must be denied. The SIM is also responsible for keeping proper documentation for employees and individuals subject to NDIs, including the date when the individual was given the NDI and by whom. A copy of all executed agreements and acknowledgements are to be provided to the PA DISO and Third Party SIM. Original executed NDAs shall be forwarded to the CISO, by the DISO, for filing in the official Port Authority records repository, with a copy to Law Department DISO.

3.6 Unauthorized Disclosure of Information

If employees, consultants, third-party contractors, or other individuals and/or entities with authorized access to Protected Information become aware that Protected Information has been released to unauthorized persons, lost, stolen or compromised, they are required to immediately notify the DISO, CISO, the Office of Inspector General, and any other appropriate information security officer and report the discovery. In the case of SSI, the CISO must inform the TSA, DOT, or USCG and, in the case of CII, the Department of Homeland Security ("DHS"), of the breach of security. DOT, DHS, TSA and USCG rules govern the reporting of any unauthorized disclosure of SSI or CII.

3.7 Security Clearance and Access Prohibitions

Access to Protected Information is not a right, privilege, or benefit of contracting with or employment by the Port Authority, rather it is based on pre-established guidance. Protected Information should not be divulged, released, turned over, or provided to any individual in any organization who does not meet the established criteria or conditions set forth herein, or who has not been approved for a security clearance issued by the Port Authority DISO, CISO or OIG. The following security clearance and access guidelines and/or prohibitions are in effect to protect Protected Information:

- Protected Information shall only be used in the performance of required job responsibilities, or in order to complete assigned tasks as determined by the SIM and DISO, with the concurrence of the CISO or OIG. No other disclosure or use of Protected Information is authorized.
- Individual access to Protected Information will be rescinded when an employee, consultant, third-party contractor, individual or entity, who had been granted access to Protected Information, is no longer employed by the Port Authority, or is no longer under contract with, or no longer has a relationship with the Port Authority, or is no longer in a position that requires access to Protected Information in order for the individual or entity to perform duties or complete tasks/projects.
    - Employees may not unilaterally sponsor themselves for background verification or enter their name on an Authorized Personnel Clearance List.
    - Group access of organizations to Protected Information should be prohibited. Each individual in a group must have security clearance to access Protected Information.
    - Persons who rarely, if ever, require access to Protected Information, (i.e., maintenance, food service, cleaning personnel, vendors and other commercial sales, or service personnel, who perform non-sensitive duties), should not be approved for a security clearance.

3.8 Background Screening

In order to determine if any individual poses a potential security threat to the Port Authority or its Facilities, the Port Authority requires background screening to verify the personal identity of, and determine the criminal history of, all contactors and consultants working in secure areas at Port Authority facilities or handling security related Protected Information. As such, employees of third party contractors/consultants requiring access to certain Protected Information relating to security on a specific project must obtain clearance through a background check prior to being provided access to information unless otherwise waived in writing by the CISO or OIG. This

includes all individuals working on the project, including administrative and back-up staff that have access to and/or are handling Confidential or Confidential Privileged Information.

All background checks for third parties required under the Policy should normally be conducted through the "Secure Worker Access Consortium" (SWAC), which is presently the only Port Authority approved service provider of a background screening checks, except as otherwise required by federal law and or regulation. The Office of Emergency Management administers this provider. S.W.A.C. is accessed by an online application (http://www.secureworker.com) that enables the secure collection, processing, maintenance and real-time positive identity verification (PIV) of individuals. The S.W.A.C. background check is not a replacement for any federal agency (DHS, TSA, etc.) required background screening. S.W.A.C. membership is valid for three years, at the end of which the member must renew the online application. In addition, certain employees, such as those in the Public Safety Department, will have their criminal history background checked through the electronic databases maintained by federal and/or state law enforcement agencies when required as a condition of employment, or when required by federal or state laws, rules, and/or regulations, or, in certain cases, where it is legally permitted and is deemed appropriate by the CSO or OIG.

The DISO/SIM has authority to obtain the background check information from S.W.A.C. Additional information about S.W.A.C., corporate enrollment and online applications can be found at http://www.secureworker.com, or it may be contacted at (877) 522-7922. The S.W.A.C. application process is described in Appendix "E."

In some cases TSA's Transportation Workers Identifications Credentials (TWIC) or Security Identification Display Area (SIDA) background screening and credential may be used in lieu of the SWAC process with approval by the DISO.

3.9 Authorized Personnel Clearance List

The DISO and SIM are responsible for compiling, maintaining, and updating their respective list databases on an ongoing basis and forwarding the information to the CISO for compilation into a master listing. Each DISO shall periodically review its department's/business unit's list with its SIM to ensure that the list is current and that each individual's access to Protected Information is still required. The CISO will maintain a master list database containing the names of all employees, consultants, third-party contractors, and other individuals and/or entities that have been granted a Port Authority security clearance and the specific category for which the security clearance was received, including, but limited to, for a particular project, or for specific Protected Information.

3.10 Development of a Confidential Information Practices and Procedures (CIPP)

Departments, offices and/or business units may adopt an individualized, discrete CIPP tailored to their respective particular business practices for handling Protected Information. The CIPP is meant to augment the Handbook and must be consistent with it. Each CIPP must be approved by the CISO before being implemented.

3.11 Procurement Strategies

(a) General

As a public agency, the Port Authority has an established procurement process based on openness, integrity, and fairness to the vendor community. The security of Protected Information must be incorporated at the beginning of the procurement process in order to establish a security benchmark that may be applied throughout the procurement process, as well as during the term of the award/contract.

(b) Lifecycle Phases and Procurements

A project may contain Protected Information in one or more of its lifecycle phases (pre-award, award, design, construction, close-out, or maintenance/service operation contracts, etc.).

Procurement and lifecycle information should be thoroughly reviewed by the originator before being submitted to the Procurement Department for processing. If Protected Information is discovered thereafter by Procurement, or any reviewing department, the originator's department manager or designee should be contacted immediately to retrieve the Protected Information and process it in accordance with the Policy and this Handbook.

(c) Risk Exposure and Business Risk Strategy

Procurement shall develop and retain, by project, a current listing of pre-screened persons or pre-qualified firms to bid on sensitive projects who agree to abide by the Policy requirements. Requirements must be included in procurement documents in order to help reduce potential disclosure of Protected Information and to provide bidders with certain security requirements in advance. They must also be included in contract awards to ensure information protection practices, procedures, and protocols are included in each project's lifecycle phase. The typical requirements are:

> **(i) Non-Disclosure and Confidentiality Agreements (NDA)**. Require prospective consultants, prime vendors, general contractors, or commercial enterprises to enter into a NDA with the Port Authority before obtaining a copy of a RFP. NDAs should be project and procurement specific and should be completed in a timely manner for specific types of procurements or projects. A broad or generic NDA should not normally be utilized to cover all procurements and projects under contract to a particular consultant, prime vendor, general contractor or commercial enterprise over a long period of time, however, it may be appropriate in certain situations to utilize such a NDA, if approved by the DISO with the concurrence of the CISO. Consultants, Prime Vendors, General Contractors, or Commercial Enterprises should contact the Port Authority to request authority prior to releasing RFP Protected Information to a sub-contractor. The sub-contractor may have to execute an Acknowledgement that it will comply with the terms of any NDA that the successful bidder has executed.
>
> **(ii) Background Screening**. Require potential users seeking access to certain Protected Information to undergo background pre-screening. The pre-screening may parallel the screening requirement used by the Port Authority to grant access to Protected Information under Section 3.3. S.W.A.C.'s background screening is usually finalized within five to ten business days.

(iii) Designation of a Security Information Manager (SIM). Require companies involved in Protected Information procurements or projects to designate a SIM to ensure information security and Protected Information requirements are followed. A second employee may be designated as an alternate SIM. All SIM"s will be required to get SWAC'd.

(iv) Information Security Education and Awareness Training. Require consultants, vendors, contractors and commercial enterprises to attend training to ensure security awareness regarding Port Authority information.

(v) Physical Security. Outline the specific guidelines and requirements for the handling of Protected Information to ensure that the storage and protection of Protected Information is consistent with the requirements of Chapter 4 of this Handbook.

(vi) Transfer or Shipping Sensitive Information. Prohibit or place restrictions on the transfer, shipping, and mailing of Protected Information consistent with the handling procedures set forth in Chapter 4 of this Handbook.

(vii) Website Restrictions. Prohibit posting, modifying, copying, reproducing, republishing, uploading, downloading, transmitting, or distributing Protected Information on unauthorized websites or web pages. This may also include restricting persons, who either have not passed a pre-screening background check, or who have not been granted access to Confidential Information, from viewing such information.

(viii) Destruction of Documents. Require Protected Information to be destroyed using certain methods, measures or technology consistent with the requirements set forth in Chapter 4 of this Handbook.

(ix) Use of Similar Agreements Between Prime Vendor and Subcontractors/Subconsultants. Require the prime vendor, general contractor, or consultant to mandate that each of its subcontractors/sub consultants maintain the same levels of security required of the prime vendor, general contractor, or consultant under any Port Authority awarded contract.

(x) Publication Exchanges. Prohibit the publication, exchange or dissemination of Protected Information developed from the project or contained in reports, except between authorized vendors, subcontractors and subconsultants, without prior approval of the Port Authority. Requests for approval should be routed to and reviewed by the CISO in conjunction with the Law Department and, where appropriate, Public Affairs.

(xi) Information Technology. Matters involving information technology policy, or use of particular hardware or software, should require the application of specific protocols and/or software tools to support Port Authority projects. Coordination of information technology and consultation with the Director of Technology Services Department and the CISO may be required for the success of particular projects.

(xii) Audit. Include provisions to allow the Port Authority to conduct audits for compliance with Protected Information procedures, protocols and practices, which may include, but not be limited to, verification of background check status, confirmation of completion of specified training, and/or a site visit to view material storage locations and protocols.

(xiii) Notification of Security Requirements. Advise all consultants, third-party contractors, and other individuals and/or entities, as may be appropriate, that Port Authority security procedure requirements may be imposed throughout the duration of the project.

(xiv) Reproduction/Copies. Reproductions of Protected Information shall be consistent with the requirements of Chapter 4 of this Handbook.

CHAPTER 4 – MARKING, HANDLING, STORAGE, TRANSMITTAL AND DESTRUCTION REQUIREMENTS

4.1 Marking of Certain Protected Information

(a) Confidential Privileged and Confidential Information

All documents, drawings, and all other Information that contain Confidential Privileged, or Confidential Information must be marked with the appropriate respective protective marking: “CONFIDENTIAL PRIVILEGED” (alternatively “CONFIDENTIAL AND PRIVILEGED”) or “CONFIDENTIAL” (alternatively, where appropriate, Confidential Proprietary Information). The markings must be conspicuous and in bolded Arial with a 16 point font size or equally visible typeface.

The front page (or front and back cover, if appropriate) shall be marked at the top and bottom of the page. In addition, all interior pages within the document must also be marked at the top and the bottom of the page. Sets of documents large enough to be folded or rolled must be marked or stamped so that the marking is visible on the outside of the set when it is rolled or folded. The marking must be visible from the exterior container of the material, e.g., the spine of a binder, or compact disc container or cover.

All Confidential Privileged Information must bear the following warning sign on its front cover, back cover, and title sheet or first page. For compact discs, DVDs or other smaller materials, the warning sign may be printed on an adhesive label and affixed to the material. It should be in visible typeface and state:

> "WARNING”: The attached is the property of The Port Authority of New York and New Jersey (PANYNJ). It contains information requiring protection against unauthorized disclosure. The information contained in the attached document cannot be released to the public or other personnel who do not have a valid need to know without prior written approval of an authorized PANYNJ official. The attached document must be controlled, stored, handled, transmitted, distributed and disposed of according to PANYNJ Information Security Policy. Further reproduction and/or distribution outside of the PANYNJ are prohibited without the express written approval of the PANYNJ.
>
> At a minimum, the attached will be disseminated only on a need to know basis and, when unattended, will be stored in a locked cabinet or area offering sufficient protection against theft, compromise, inadvertent access and unauthorized disclosure.

(b) Sensitive Security Information Requirements

Pursuant to the federal regulations governing SSI, Port Authority Protected Information that has been designated SSI by the Federal government must be conspicuously marked with its respective protective marking “SENSITIVE SECURITY INFORMATION” on the top and the distribution limitation statement on the bottom of each page of the document including, if applicable, the front and back covers, the title page, and on any binder cover or folder. The

protective marking must be in bolded Arial 16-point font size and the distribution limitation statement must be in an 8-point font size. All copies of SSI documents must also bear the required markings.

The distribution limitation statement is:

> WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the TSA or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

(c) Critical Infrastructure Information

Pursuant to the federal regulations governing CII, Port Authority Protected Information that has been marked PCII by the Department of Homeland Security PCII Program Manager or the manager's designee will be marked as follows:

> This document contains PCII. In accordance with the provisions of 6 CFR Part 29, this document is exempt from release under the Freedom of Information Act (5 U.S.C. 552 (b)(3)) and similar laws requiring public disclosure. Unauthorized release may result in criminal and administrative penalties. This document is to be safeguarded and disseminated in accordance with the CII Act and the PCII Program requirements.

(d) Document Control Number for Confidential Privileged Information

Documents that have been identified as Confidential Privileged Information will be given a control number, which shall consist of the category of information followed by an acronym for the transmitting department, followed by the last 2 digits of the year, followed by a number that is sequential and, finally, followed by the copy number.

Examples:

CP – LAW – 13 – 1 – 1

CP – PMD – 07 – 10 – 2

The front page (or front and back cover, if appropriate) and all pages of Confidential Privileged Information shall be marked with the control number. The control number must also be visible from the exterior container of the material, e.g., the spine of a binder, or compact disc container or cover. If deemed necessary by the DISO or CISO, certain Confidential Information or other Protected Information may be given a control number.

4.2 Handling Protected Information

Handling refers to the physical possession of, and includes working on or with, Protected Information to perform job duties or complete tasks or projects. This includes, but is not limited to, reading, copying, editing, creating, or correcting the material. Protected Information in any form, including physical or electronic, must be under constant surveillance by an authorized individual to prevent it from being viewed by, or being obtained by, unauthorized persons. Protected Information is considered to be in use when it is not stored in an approved security container.

The following is a chart of the minimum-security requirements for handling Protected Information, and certain requirements that apply only to Confidential Privileged and Confidential Information:

Minimum Security Requirements for Handling	**Confidential Privileged Information**	**Confidential Information**
Must never be left unattended outside of storage location.	X	
Must be under the direct and constant supervision of an authorized person who is responsible for protecting the information from unauthorized disclosure.	X	
Must be turned face down or covered when an unauthorized person is in the vicinity. Be cognizant of others in area that can view your computer screen.	X	X
When leaving a computer unattended ensure that the screen is locked.	X	
Attach an information cover sheet when removing materials from their place of storage.	X	
Use all means to prevent unauthorized public disclosure of information.	X	X

4.3 Transmittal of Protected Information

Transmission refers to the sharing among individuals and/or entities, and/or the transfer or movement of Protected Information from one location to another using either physical or electronic means. The following chart sets forth the methods by which Protected Information should be transmitted. In all instances, Protected Information must at all times be safeguarded and transmitted in a manner and method designed to insure that it is not disclosed, or otherwise compromised, and it should be appropriately marked with the proper identifying marking.

In general, all Confidential Privileged Information must be signed in and out, and, in certain situations as determined by the DISO or SIM, Confidential Information may be signed in and out as well. A cover sheet must be attached to the Confidential Privileged or, in certain situations as determined by the SIM, to Confidential Information and it should be marked appropriately. With respect to Confidential Privileged Information, the coversheet attached as Appendix "F" is to be utilized to draw emphasis to the fact that a document contains Confidential Privileged Information and to limit visual exposure to unauthorized individuals in near proximity. Confidential Privileged Information and, where appropriate, Confidential Information, must be wrapped and sealed. The exterior of the wrapping should not indicate that it is sensitive material, or its category, or level.

Confidential Privileged Information may be transported using public modes of transportation, and a courier service may also be utilized; provided, however, that the sign in and sign out procedures will apply, as well as wrapping and sealing procedures. All packages must be sealed in a manner that easily identifies whether the package has been opened prior to delivery to the intended recipient. The use of a double wrapped/enveloped package or a tamper resistant envelope must be used to fulfill this requirement. Protective markings are not to be placed on the outer visible envelope. If using a double wrapped package or two envelopes, the inner wrapping or envelope should be marked in accordance with appropriate category designation. The package must be addressed to an individual who is authorized to receive it or, preferably, to the SIM. All packages must contain a specific individual's name on the shipping label. Where appropriate any of the foregoing requirements may also be required in handling Protected Information and can be provided for generally in the department's CIPP, or as required by the DISO and/or SIM with respect to handling such information in specific instances.

Minimum Security Requirements for Transmission	**Confidential Privileged Information**	**Confidential Information**
Verbally at a meeting, conference or briefing where all attendees have the appropriate security clearance	X	X
Electronic Systems: restrict to Livelink[2] or a similar approved secure repository	X	
Electronic Mail: restricted from using e-mail accounts to transmit. NOTE: Confidential Information may be transmitted using encryption with express permission by the DISO/SIM, in writing	X	
Hand Carried or delivered in the personal custody of Authorized Individual: (a) request return receipt (b) place in sealed envelope, and (c) name of recipient, department, address and phone number must be written on face of envelope	X	X (b and c only)
Approved Commercial Delivery Service (e.g., DHL, FedEx, UPS): (a) request return receipt, (b) verify recipient name and mailing address, (c) place in a sealed envelope, and (d) the		

[2] Livelink is a secure collaborative repository for the documents of a project.

exterior of a mailing document shall not indicate the security category of the material contained therein	X	X
Use of USPS Certified Mail: (a) request return receipt, (b) verify recipient name and mailing address, and (c) the exterior of a mailing document shall not indicate the security category of the material contained therein	X	X
Intra-agency Mail System (a) request return receipt (b) place in sealed envelope, (c) name of recipient, department, address and phone number must be written on face of envelope, and (d) the exterior of a mailing document shall not indicate the security category of the material contained therein	X	X (b, c, d only)
Telephone: restricted from using a non-land line telephone to transmit, unless expressly permitted by SIM in writing. If approved: (a) use all means to prevent unauthorized public disclosure, and (b) may not use mobile or internet devices.	X	
Fax Machine: restricted from using fax machine to transmit unless expressly permitted by the SIM in writing. If approved: (a) prior coordination with recipient required, (b) verify recipient fax number, (c) receipt of successful transmission, and (d) follow-up contact required	X	X (a,b,c only)

Steps for transmittal of a “hard copy” of all Confidential Privileged Information and, when required, for Confidential Information:

Step 1. Make certain that documents are properly marked: “CONFIDENTIAL PRIVILEGED,” or “CONFIDENTIAL,” according to its designated category.

Step 2. Prepare Transmittal Receipt (Appendix “F”).

Step 3. Place document in envelope with the Transmittal Receipt, seal envelope, mark the inner envelope CONFIDENTIAL PRIVILEGED or CONFIDENTIAL, place envelope in second envelope (outer), this envelope shall not contain any protective markings.

Step 4. Address envelope to an individual who is authorized to receive it.

Step 5. Mail document.

Step 6. The Transmittal Receipt shall be returned to the party who initially sent the item.

When hard copies of 8 1/2 ” X 11” multi-page documents include threat scenarios, asset criticality information, identification of security vulnerability details, risk assessments, design basis threats and concepts of operations are distributed, this information is to be bound using secure binding to prevent individual sheets from being removed from a set.

4.4 Storage of Protected Information

Steps should be taken to prevent unauthorized access to Protected Information. Certain Protected Information should be kept in a locked storage room or a locked security container, such as a drawer, cabinet or safe-type file that has a locking mechanism, and must be vandalism resistant. The DISO will periodically review the departmental storage vehicles and mechanisms and determine their appropriateness for the information being stored. Protected Information should be gathered and stored in a minimum number of office locations. Confidential Privileged Information must never be left unattended outside its storage location for long durations. A storage space or security container/receptacle may not be left open and unattended at any time. At no time should Confidential Privileged or Confidential Information be stored, except for short periods during work, in unauthorized desk drawers, file cabinets, or other unsecured locations. The CISO may require that certain information be kept in a safe in a designated central location(s).

Combinations or locks for each security container must be changed or replaced when a person having knowledge of the combination or possession of a lock key no longer requires it, leaves the project or there is reason to suspect that the combination has been tampered with, or that an unauthorized person may have acquired knowledge of the combination, or that a lock key is in the possession of an unauthorized person. Keys and combinations of locks utilized to secure certain Protected Information must be safeguarded at the same level of protection as paper documents. The "Guidelines for the Storage of Confidential Privileged, Confidential and Law Enforcement Confidential Information" attached as Appendix "H" provides further detailed information and instructions.

Confidential Privileged Information and, where appropriate Confidential Information, may not be stored at any individual's home overnight for a meeting the following day without prior written authorization of the SIM or DISO.

Downloading of any Confidential Privileged Information and Confidential Information carries with it the responsibility to protect that information in accordance with the procedures identified in this Handbook. The possessor of the electronic file assumes full responsibility for the proper handling, storage, transmittal and disposal of this Confidential Privileged and Confidential Information.

4.5 Document Accountability Log

All entities, Port Authority Departments and third-parties having Protected Information in their possession will have a system in place that will account for the material in such a manner that retrieval is easily accomplished for inspection. The accountability log with respect to Confidential Privileged and Confidential Information shall be maintained by the DISO, or the SPM, or SIM, where applicable, and include:

- The date that a document was received or created
- The identity of the sender or creator
- A brief description of the document
- The Control Number, if Confidential Privileged Information
- Number of copies

- Transmission history (sent to whom, when)
- If applicable at the time of the inspection, a Port Authority Document Destruction Certification, stating that the document has been destroyed (including, when, by whom and the method), or a Certification that the document has been returned to the Port Authority.

4.6 Reproduction

Protected Information should only be reproduced to the minimum extent necessary to carry out an individual or entity's responsibilities. However, the reproduced material must be marked and protected in the same manner and to the same extent as the original material. Authorized individuals must perform all reproduction work. Print and reproduction locations are limited to Port Authority sites, or, when appropriate, to authorized consultant and/or third-party contractor work site equipment. The CISO may require that the work site should limit reproduction of Protected Information to a particular copying machine with technological capabilities limited to copying (not scanning or storing etc.). Service providers, authorized by the responsible SIM or DISO where appropriate, may be used for this task if the information remains safeguarded throughout the process. Each reproduction of Protected Information shall contain all security markings, instructions, etc., as set forth in Section 4.1. All scraps, over-runs, and waste products resulting from reproduction shall be collected and processed for proper disposal.

4.7 Destruction of Protected Information

All Protected Information that is no longer needed shall be disposed of as soon as possible, consistent with the Port Authority's Record Retention Policy, by any method that prevents its unauthorized retrieval or reconstruction. Authorized service providers may be used for this task provided that the information remains safeguarded until the destruction is completed. Paper products must be destroyed using a cross cut shredder located in the office. As previously noted in Section 4.5, a Port Authority Document Destruction Certificate must be provided to the DISO or SIM for any document being destroyed, including original or copies thereof. In addition to the requirements in this Handbook, all Departments shall continue to comply with the Port Authority Records Program (A.P. 15-2.02). Where Protected Information is no longer needed, but the Port Authority Records Program requires retention of the original, the original Protected document shall be retained by the Departmental Records Coordinator and all copies are to be destroyed in accordance with this section. The "Guidelines for the Disposal and Destruction of Confidential Privileged Information" attached as Appendix "I" provides further detailed information and instruction.

Since deleted electronic files can be recoverable by utilizing software tools, certain Protected Information stored in electronic form needs to be erased and destroyed with methods that comply with the US Department of Defense standards for file secure erasure (DoD 5220.22). Therefore, CyberScrub or a similar software shall be used to prevent discovery by a computer technician or other unauthorized person. With respect to Port Authority staff, individual staff shall contact the Technology Services Department ("TSD") to make a request that Protected Information be permanently removed from a computer. This request shall be made by providing relevant information on a TSD Service Request (TSR), found on eNet on the TSDpage.

4.8 Information Technology Systems – Handling of Electronic Information/Data

All transmission, storage and destruction of all electronic information and data must be in compliance with the Technology Services Department's (TSD) "Cyber Security Guidelines for the Port Authority of New York and New Jersey"

Information Technology (IT) Systems that are used to electronically capture, create, store, process or distribute Protected Information must be appropriately managed to protect against unauthorized disclosure of the contents. The main objectives of these electronic handling guidelines are to:

- Provide access exclusively to the authorized individuals.
- Compartmentalize Protected Information as required by a Department's CIPP.
- Complete removal of Protected Information from the system when it is no longer needed.

This section is intended to describe the processes used to control secure electronic data, and is to be implemented for the control, processing, handling, storage, and destruction of all "Protected" electronic data as generated, received, or distributed by Authority staff, consultants, contractors or third parties.

4.9 Transmission/Exchange of Electronic Information

The Authority uses Livelink (moving toward PACS) as its project and program website solution to collaborate with team members (i.e., authorized individuals) both inside and outside the Agency's firewall. Additionally, the Authority also uses secure internet websites with secure transmission to collaborate with team members outside the Agency. The use of a web-based collaboration tool has numerous benefits that result s in time and cost savings, accountability, security, and disaster recovery. For example, within the Authority, the Downtown Restoration Program (DRP), the Security Capital Program, Office of Emergency Management, and the Goethals Bridge Program, utilize Livelink website collaboration.

Access to these password-protected websites is controlled by permissions that apply to each individual user account. In this manner, users are allowed to access folders and files only when approved by the SIM, Project Manager or Program Manager directly responsible for the information.

With these measures in place, the Authority has deemed that all electronic exchange of Protected Information must be accomplished using a secure project website solution with centrally managed access control on a per individual basis and with encrypted transfer.

Although the entire Port Authority Website is secure, in order to provide better organization and auditing of files that contain Confidential Privileged or Confidential Information, special secure folders must be created and maintained specifically to house this information. Information that has been designated as Confidential Privileged Information may only reside in these secure folders in order to further compartmentalize it from other types of information.

Additional secure Protected Information folders will allow other files such as reports, presentations, etc., to be stored.

In addition to the Livelink website, certain electronic Protected Information may also be shared via secure Local Area Networks (LAN). Protected Information should be removed from the LAN as soon as the recipient has acknowledged receipt of the information. As with the website, these LANs are password protected, and access to them is only for those individuals who have signed the NDA and are provided with permission by the SIM or DISO, if required.

E-mailing of Confidential Privileged Information is not permitted, E-mailing of any other Protected Information must be encrypted as per TSD standards.

4.10 Electronic Storage

Technology advances allow increasingly larger amounts of information to be stored on increasingly smaller devices. This creates a greater risk of information security breaches due to the size and portability of these devices, which can be lost or misplaced more easily when taken outside of the office. If a situation arises whereby electronic files must be exchanged by electronic media such as flash drives, CD or DVD, all provisions within this manual for handling physical documents must be satisfied.

Possession of Protected Information in any format (hardcopy, electronic, photo, video, etc.) carries with it the responsibility to protect that information in accordance with the requirements of the Handbook. Authorized individuals in possession of electronic files containing Protected Information assume full responsibility for the proper handling, storage, transmittal, and destruction of this type of information in the same or comparable manner as hard copy requirements.

Users who possess electronic files containing Protected Information shall adhere to the following guidelines to maintain the proper protection of this material:

Desktops/Laptops/CAD Machine Users

Individuals granted access to The Port Authority Network or information systems shall secure computers from unauthorized access.

- When leaving a computer unattended, users shall apply the “Lock Workstation” feature (ctrl/alt/delete, enter).
- Unattended computers shall be secured from viewing by password protected screen savers.
- Computers shall activate the automatic screensaver feature after a period of non-use. The period of non-use is fifteen (15) minutes, or a shorter time period if required by a DISO.
- Desktop computer users shall only store Confidential Privileged and Confidential Information on a secure password protected network drive (directory on The Port Authority Network) and not the computer’s local hard drive.
- Laptop computer users shall store Confidential Information locally, when necessary, with encryption software. Users shall contact their respective DISO to request or confirm that Port Authority standard encryption technology is installed on their assigned laptop computer.
- Computer users shall not disable or alter security safeguards, such as virus detection or encryption software, installed on Port Authority computers.

Portable Media

- Confidential Privileged Information shall be encrypted on portable devices, including handheld devices, if they are carried outside secure worksites.
- All Protected Information stored on portable devices shall be password protected at the document level.
- Mobile laptop computers, computer media and any other forms of removable storage (e.g., diskettes, CD ROMs, flash drives) shall be stored in a secure location or locked cabinet when not in use.

4.11 User Access Deactivations

In addition to accessing the IT Systems, Port Authority, through the appropriate Systems Administrator, may deactivate a User's IT privileges, whether or not the user is suspected of any violation of this Policy, when necessary to preserve the integrity of facilities, user services, or data.

CHAPTER 5 – AUDITING AND MONITORING

5.1 Purpose

The ISSC, Audit and/or OIG may conduct random or scheduled examinations of business practices under the Policy in order to assess the extent of compliance with the Policy. The Policy's self-assessment and audit processes enable management to evaluate the Policy's uniformity throughout the Port Authority and of third parties' practices, in order to identify its strengths and potential exposures, and to help guide evolving policy objectives.

5.2 Audits and Investigations

Audits conducted by the ISSC, Audit, and/or OIG may be scheduled in advance. The chief, department director, project manager, company liaison or contract representative of the organization being assessed should receive prior notice of the date of the assessment and also be advised as to what the assessment will consist of. A copy of the current version of the Audit Procedures guidelines, attached as Appendix "J", should be provided to the particular entity(ies) in order to allow adequate time to undertake appropriate pre-review and preparation action. The Audit Procedures guidelines should guide the ISSC and/or Audit through the assessment process. This Guideline is not all-inclusive and may be amended, as necessary. Organizations, departments, units, or third parties, preparing for an ISSC and/or Audit visit are encouraged to contact the CISO prior to the scheduled visit date in order to inquire and obtain additional information about the process.

The ISSC and/or Audit may also conduct information security assessments without prior notice and/or unannounced investigations coordinated through the Office of the General Counsel and the Office of Inspector General, as it may deem necessary and appropriate. Where appropriate, the CISO should be advised of the existence of such an investigation and, if appropriate, its nature.

The ISSC and/or Audit approach to conducting an assessment should consist of three phases (i) personnel interviews, (ii) site assistance visits, and (iii) corrective action follow-up.

(i) Personnel Interviews

The interview(s) should focus on the department, business unit, organization or third party's compliance with the Policy, how engaged the interviewee is with the Policy, and the level of education and awareness the interviewee has about the Policy. Employees, consultants, third-party contractors, and other individuals and/or entities should be included as potential interviewees. Personnel interviews should encompass a wide range of individuals who are regularly engaged with the Policy, as well as those having less involvement in it. This allows the ISSC to develop a balanced understanding regarding Policy compliance and effectiveness, as well as its impact on the organization and enable it both to identify concerns and issues regarding the Policy, and to solicit recommendations for possible improvements to the Policy.

(ii) Site Assistance Visits

The ISSC and/or Audit site visit should focus on a hands-on review of the following processes and procedures: document safeguards, handling protocols, transmission practices, control number usage, document marking, receipt and copying practices, and disposal of Protected Information procedures. The visit should also include compliance reviews of the security clearance access criteria, document accountability audits, conditions regarding information access, background check processes, Authorized Personnel Clearance Lists updates, Protected Information material sign out and sign in records, where appropriate, and the information security education awareness training program.

(iii) Follow-up

Policy compliance deficiencies noted during the assessments should be provided by the ISSC and/or Audit through the CISO to the department head, chief, project manager, consultant, third-party contractor liaison/representative, other agency staff, and the respective DISO or SIM for corrective action. The ISSC, through the CISO, may also follow-up on investigation results to determine corrective actions and Policy compliance. The ISSC may also recommend the imposition of any penalties or disciplinary action that are described in Chapter 6.

With the assistance of the respective DISO or SIM, a plan with milestones should be developed with the intention of correcting any identified deficiencies. A return site assistance visit may be scheduled in order to re-assess earlier identified deficiencies. The respective DISO, SPM, or SIM should forward a periodic corrective action progress report to the CISO as part of the milestone monitoring.

5.3 Self-Assessment

Department heads, chiefs, managers, supervisors, DISOs or SIMs should conduct an annual self-assessment of their unit's Policy compliance using the Audit Procedures Guidelines. The results will not be forwarded to the CISO, Audit or ISSC, but should be used as a tool to gauge compliance before regular assessments are conducted. The results should be available for inspection and any serious findings should be forwarded to the CISO.

CHAPTER 6 – POLICY VIOLATIONS AND CONSEQUENCES

6.1 Responsibilities

Anyone having knowledge of any infraction, violation or breach of the Policy is required to report it to the CISO, OIG, their DISO, and third party SIM, who shall in turn report the same to their supervisor/manager. The CISO shall have the final decision with respect to the violation determinations and/or the recommended course of action to be taken, consistent with Port Authority policy, practices and legal requirements referenced in this section.

All individuals who have been reported as having violated the Policy may be temporarily denied access to Protected Information and/or have their security clearance suspended until an investigation is completed.

6.2 Violations, Infractions, or Breach of Information Security Protocols

Due to any number of unintended circumstances or, other conditions beyond the control of an individual, Protected Information could be subject to compromise or loss. For example, an individual may unintentionally discard Protected Information, mislabel Protected Information, sent through the internal mail routing system, or drop or inadvertently leave Protected Information in a public place. Intentional disclosure of Protected Information to unauthorized individuals for personal gain, or to otherwise make available for unauthorized public release, may also occur. Violations, infractions and breaches of the Policy will be reviewed on a case-by-case basis to determine the facts and circumstances surrounding each incident.

6.3 Violation Reporting, Investigation and Fact Finding

Individuals must report alleged or suspected violations, infractions or breaches of the Policy to the DISO, CISO, OIG and to their supervisor or manager. The DISO, in consultation with the CISO and OIG, will determine whether an investigation into the allegations or other appropriate action is warranted. The CISO will consult with the OIG on these matters and the OIG will determine whether to undertake its own separate investigation into the matter. Individuals and/or entities must cooperate with all authorized investigations of any act, omission or occurrence relating to Port Authority property, information, materials, and, in the case of Port Authority employees, and if applicable, must comply with the Agency General Rules and Regulations. (See *"General Rules and Regulations for all Port Authority Employees."* Port Authority of New York and New Jersey. April 1990.)

6.4 Disciplinary Action

The following is a list of Policy violations and the possible respective disciplinary actions that may be taken against any individual and/or entity, having authorized access to Protected Information, who violates their responsibilities in handling such information:

a) Non-deliberate violations involving negligence and/or carelessness, such as leaving Protected Information unattended.

First Offense: Verbal reprimand and security briefing.

Second Offense: Written reprimand and/or a security briefing and possible suspension or termination of access privileges, depending on the circumstances.

Third Offense - Termination of access and possible imposition of civil penalties. Where the offense involves a Port Authority employee, disciplinary action may also be taken.

b) Non-deliberate violation involving negligence and/or carelessness such as misplacing or losing a document.

First Offense - Written reprimand and/or a security briefing, and possible suspension or termination of access privileges, depending on the circumstances, and possible imposition of a civil penalty. Where the offense involves a Port Authority employee, disciplinary action may also be taken.

Second Offense - Dismissal or termination of access privileges, and, depending on the circumstances, the imposition of a civil penalty, and possible legal action against the violator. Where the offense involves a Port Authority employee, disciplinary action may also be taken including suspension with forfeiture of up to one year's personal and vacation time allocation.

c) For cases of deliberate disregard of security procedures or gross negligence in handling Confidential Privileged and Confidential Information.

First Offense – Suspension or termination of access privileges, termination of an agreement or contract, written reprimand, imposition of a civil penalty depending on the circumstances, and possible legal civil and/or criminal action against the violator. Where the offense involves a Port Authority employee, disciplinary action may be taken up to and including termination of employment. Termination of access privileges will be for a period of one year at minimum and may be permanent, subject to review by the CISO.

The Port Authority may also impose investigation costs and/or a monitor to oversee future compliance with its security policies and practices at the violator's expense, when the violation is by a consultant, vendor contractor or other third party. Nothing herein is construed to limit the Port Authority's right to exercise or take other legal rights and remedies including terminating agreements with a third party violator and/or refusing to enter into future business relationships with the violator and/or seeking such legal action, as it may deem appropriate, including injunctive, civil actions for monetary damages and/or seeking criminal prosecution of the violator(s).

In addition, any violation relating to SSI or CII will be reported to the TSA, the OIG, and/or, if applicable, DOT, USCG or DHS. Penalties and other enforcement or corrective action may be taken as set forth in relevant statutes, rules and regulations, including, without limitation, the issuance of orders requiring retrieval of Sensitive Security Information and Critical Infrastructure Information to remedy unauthorized disclosure and directions to cease future unauthorized disclosure. Applicable Federal Regulations, including, without limitation, 49 C.F.R. § 15.17 and 1520.17 and 6 CFR Part 29, provide that any such violation thereof or mishandling of information therein defined may constitute grounds for a civil penalty and other enforcement or corrective action being taken by the DOT, TSA and/or DHS.

CHAPTER 7 – INFORMATION SECURITY EDUCATION AND AWARENESS TRAINING

7.1 Purpose

Information Security Education and Awareness training ensures that all personnel requiring access to Protected Information, regardless of position or grade level, have an appropriate understanding of the need to adhere to security procedures in order to secure Protected Information. The goal of the training program is basically to provide that all such employees, consultants, third-party contractors, other individuals, entities and/or, where appropriate, third parties develop essential security habits and thereby ensure that all personnel accessing Protected Information understand and carry out the proper handling protocols for those materials.

7.2 Overview

The CISO is responsible for implementing the Information Security Education and Awareness Training Program (the "Training Program"). The Training Program, with assistance from the Office of Inspector General, DISO and SIM, should be provided to all employees, consultants, third-party contractors, and other agency personnel requiring access to Protected Information. These individuals, regardless of rank or position in a particular organization, must complete initial indoctrination and refresher training. The CISO, with the concurrence of the Law Department, may waive this requirement for certain individuals. A current list containing the names of all persons who completed training will be developed and retained by the CISO. The CISO shall ensure that all employees have complied with the requisite Training Program.

7.3 Training Program Elements

The Training Program consists of three interconnected elements: (a) indoctrination training, (b) orientation training, and (c) refresher training, recommended every three years. Each element provides employees, consultants, third-party contractors, and other agency personnel with a baseline of knowledge, as well as periodic updates, about the existing and current Policy. Each element of the Training Program contributes another level of information to the individual. At a minimum, all individuals must receive the indoctrination training, and the refresher training, if warranted.

(a) Indoctrination Training

Indoctrination Training provides personnel with the fundamentals of the Training Program. It should be completed when beginning employment or assignment to a project for the Port Authority, but no later than sixty (60) days after initial hire, or after commencing work on a project. It may be combined with other types of new employee indoctrination programs. Individuals completing this level of training should understand the basic organization of the Policy, the Policy definitions, what materials are defined as Protected Information under the Policy, how to identify Protected Information (security category levels and markings), the general criteria and conditions required in order to be granted a security clearance, procedures for categorizing documents, the obligation to report suspected and alleged policy violations, and the penalties for non-compliance with the policy and for unauthorized disclosure of Protected Information.

(b) Orientation Training

Orientation Training focuses on the more specific protocols, practices and procedures for individuals whose roles and responsibilities involve reading, using, safeguarding, handling, and disposing of Protected Information. Individuals assigned such responsibilities should complete this level of training. Orientation training should be conducted prior to assignment to a department, project, task, or other special assignment, where the individual is expected to become involved with receiving and handling Protected Information. Individuals completing this level of training should be introduced to the DISO or SIM, understand the organizational elements of the Policy, know how to process Protected Information, know the different security categories under their control or within their assigned work environment, know how to identify proper safeguarding protocols, including hardware needs, and understand the differences between general access privileges and the need to know requirement for access to particular information. Individuals should also read and acknowledge their understanding of the requirements.

(c) Refresher Training

Within a three (3) year time period during the anniversary month of the individual's start date on a project, or initial access to Protected Information, all employees, consultants, third-party contractors, and other individuals and/or entities, who continue to have access to sensitive materials, should receive an information security education and awareness training refresher briefing to enhance their information security awareness. At a minimum, the refresher training should include indoctrination and orientation topic training, as well as key training on recent Policy changes or other appropriate information. Also, this milestone may be used to reaffirm the individual's need for a security clearance or to determine whether the individual requires a periodic update of their background check.

(d) Other Circumstances and Special Briefings

If a Port Authority employee, consultant, third-party contractor, or other individual and/or entity transfers to another department, is promoted within his or her department, or changes employers on the same project without a break in service, and can provide a record of completion of indoctrination training within the previous twelve months, only annual refresher training may be required. All other situations demand that an individual requiring access to Protected Information fulfill the conditions for information security education and awareness training under this Policy.

In addition to reading and signing a NDA or an Acknowledgment of an existing NDA, or, alternatively, being subject to a NDI, temporary or one-time access individuals should be fully briefed on the limitations on access to Protected Information and the penalties associated with the unauthorized disclosure, before being granted access to such information.

Special briefings may be provided on a case-by-case basis, as circumstances may require.

APPENDIX A
PROTECTED INFORMATION

Confidential Privileged Information

- Information that reveals security risks, threats, vulnerabilities, built –in or potential to Port Authority facilities and/or assets
- Documentation that identifies specific physical or system security vulnerabilities, when referring to specific security or terrorist threats and/or the specific capabilities in-place to counter a threat
- Documentation revealing specific security vulnerabilities at a new or existing PANYNJ facility, if specific weaknesses are reflected or maximum tolerances are provided
- Information revealing details of defeating a security system(s) or revealing the system in its entirety
- Drawings or documents that reveal specific security design criteria or ratings with regard to security performance
- Information identifying the basis for implementing an operational or technical security solution
- Details related to emergency response protocols, egress plans, flow paths, egress capacities, security systems, etc., not publicly available (diagrams, codes, standards)

Information includes, but is not limited to:

1. Security Risk and Threat Assessments (SRA);
2. Design Basis Threat Analysis (DBT);
3. Facility Security Programs/Plans (to the extent such Programs/Plans are not designated as SSI or CII);
4. Continuity of Operations Plans;
5. Security White Papers;
6. Blast Protection Design Requirements; Blast Analysis; Vector Analysis (Security Barriers, Bollards, etc.);
7. Structural plans, details and specifications if site specific information involves details regarding the capability or vulnerability of security system(s) or additional protection to a critical structure(s);
8. Drawings and/or documents with specific forced entry ratings;
9. Security System(s) designs when high technology data, which was developed by or for the Port Authority, is site specific or concerns core area system;
10. Critical element of security or life safety system; such as master controls, overrides, backup power sources when such elements would not be readily observable by the public;
11. Security system(s) command and control operating instructions and supporting countermeasures when referring to a specific site or project location;
12. Design data revealing engineering, construction of a Communication or Data Center electrical system, network connections, or facility support system with signal cable (e.g., intercom, telephone);

Confidential Information

- Specific security system/hardware model number installed at specific locations
- Details concerning overall security system(s) or individual sub systems(s), including design engineering, construction, fabrication and rollout schedule when data is site specific or concerns core area systems
- Structural plans and details if site-specific information involves details of security system(s) of protection
- Design data revealing engineering, construction, or fabrication details of primary and emergency electrical power systems supporting security, communications or life safety systems
- Documents identifying protective measures around Operations & Control Centers
- Documents identifying the location of Police and Emergency Communication Lines
- Security budget information
- Security Capital Plan
- Security personnel information

Information includes, but is not limited to:

1. Methods utilized to mitigate vulnerabilities and threats, such as identity, location, design, construction, schedule, and fabrication of security systems;
2. Details concerning overall security system(s) or individual subsystem(s), including design, engineering, construction, fabrication and rollout schedule when data is site specific or concerns core area systems;
3. Concept of Operations (CONOPS) documents;
4. Structural plans and details if site-specific information involves details of security system(s) or protection;
5. Documents identifying protective measures around Operation Control and Data Centers;
6. Documents identifying the location of Police, Emergency Communication and Network Lines;
7. Security White Papers
8. Secure Identification Display Area (SIDA) Badge Application (Aviation)
9. Selected Environmental Documents – Condition Surveys containing information on contaminated sites;
10. Emergency Operations Plan (to be shared with other Agencies);
11. Guidance for Managing Multi-Agency Response to WMD/CBREN Incidents;
12. Security system logs and reports, system operators and users including all related personal and company data;
13. System information used to construct and protect security systems;
14. Information/documents complied for law enforcement or official investigatory purposes;
15. Sensitive financial, commercial and other business information received from third parties under Non-Disclosure and Confidentiality Agreements:
16. Security Project Management budget Information;
17. Security Project Management Capital Plan;
18. Property Lease Agreements (Negotiations);
19. Legal Settlement agreements (when specified in the final settlement agreement);
20. Financial Analysis relating to ongoing litigation;
21. 5-year Capital Security Plan.
22. Law Enforcement investigatory material based upon the sensitive or confidential nature of the information

Health Insurance Portability and Accountability Act (HIPAA)

Employees, associates or other contract personnel who have access to Protected Health Information (PHI) must also refer to, and comply with, the Privacy Policies and Procedures to Protect Personal Health Information. Privacy regulations issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA" or "Privacy Laws") place restrictions on the Group Health Plans of the Port Authority and PATH (the "Plans") ability to use and disclose Protected Health Information ("PHI").

To protect the privacy and confidentiality of PHI and to comply with HIPAA, all members of Employee Benefits, including the Customer Service Representatives, and any others who have access to PHI, must comply with the policies and procedures set forth in this manual (the "Policies and Procedures"). The purpose of this manual is to establish how the Privacy Laws are to be implemented by the Plans and Employee Benefits in particular. This document maintained by the Employee Benefits Division of HRD, addresses Privacy Law Concerns related to the Health Insurance Portability and Accountability Act (HIPAA).

HIPAA defines **Protected Health Information (PHI)** as all individually identifiable health information that is transmitted or maintained by the benefit plans in any medium – electronic, oral or written. The Port Authority receives this information in its employer capacity and, therefore, it is not considered to be PHI:

- An individual's name, address, birth date, marital status, dependent information and Social Security number;
- An individual's choice of health plan;

Attorney Work Product

Attorney work product and other privileged information should be protected and treated in accordance with the established rules of the profession and may carry the marking "Privileged & Confidential". Certain work product information may also fall within the definitions of Confidential Privileged and/or Confidential Information as established by the Handbook, and as such, should be marked and treated in accordance with the Handbook and the Law Department CIPP.

Federal Designations:

Security Sensitive Information (SSI): has the definition and requirements set forth in the Transportation Security Administrative Rules & Regulations, 49 CFR 1520, (49 U.S.C. §114) and in the Office of the Secretary of Transportation Rules & Regulations, 49 CFR 15, (49 U.S.C. §40119) and any amendments thereto.

1. Facility Security Programs/Plans (Aviation and Port Facilities fall under SSI);
2. Exclusive Area Agreements (Aviation and Ports – An agreement between PA and tenant that has a security program, which permits the tenant to assume responsibility for security within the affected area(s). SSI);
3. TAS Security Directives (SSI);
4. SEA LINK Database and corresponding applications (Ports - SSI/Privacy Act Information).
5. Security Directives issued by the TSA

Critical Infrastructure Information (CII); has the meaning set forth in the Homeland Security Act of 2002, under the subtitle Critical Infrastructure Information Act of 2002 (6 U.S.C. §131-134), and any rules or regulations enacted pursuant thereto, including, without limitation, the Office of the Secretary, Department of Homeland Security Rules and Regulations, 6 C.F.R. Part 29 and any amendments thereto. CII may also be referred to as "Protected Critical Infrastructure Information" or "PCII," as provided for in the referenced rules and regulations and any amendments thereto.

PROTECTED INFORMATION (CONFIDENTIAL INFORMATION)	
Handbook Marking • **Confidential Privileged** • **Confidential** • **CII & SSI**	**Outside Handbook Marking Protocols** • **HIPAA** • **Litigation/Law** • **Law Enforcement Investigatory Material** • **Active Negotiations** • **RFP Proposals under evaluation**

APPENDIX B

Non-Disclosure and Confidentiality Agreements

B-1
Non-Disclosure and Confidentiality Agreement with reference to Handbook

NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT
BETWEEN

[1]

AND

THE PORT AUTHORITY OF NEW YORK AND NEW JERSEY

THIS NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT (this "**Agreement**") is made as of this [2] day of [3], [4], by and between **THE PORT AUTHORITY OF NEW YORK AND NEW JERSEY** (the "**Port Authority**") a body corporate and politic created by Compact between the States of New York and New Jersey, with the consent of the Congress of the United States, and having an office and place of business at 4 World Trade Center, 150 Greenwich Street, New York, New York, 10007, and [5] having an office and place of business at [6] ("**Recipient**").

WHEREAS, the Port Authority desires, subject to the terms and conditions set forth below, to disclose to Recipient Protected Information (as defined below) in connection with [7] (collectively, the "Project(s)", or "Proposed Project(s)"); and

WHEREAS, the Recipient acknowledges that the Port Authority, in furtherance of its performance of essential and critical governmental functions relating to the Project, has existing and significant interests and obligations in establishing, maintaining and protecting the security and safety of the Project site and surrounding areas and related public welfare matters; and

WHEREAS, in furtherance of critical governmental interests regarding public welfare, safety and security at the Project site, the Port Authority has collected information and undertaken the development of certain plans and recommendations regarding the security, safety and protection of the Project site, including the physical construction and current and future operations; and

WHEREAS, the Port Authority and Recipient (collectively, the "**Parties**") acknowledge that in order for Recipient to undertake its duties and/or obligations with regard to its involvement in the Project, the Port Authority may provide Recipient or certain of its Related Parties (as defined below) certain information in the possession of the Port Authority, which may contain or include protected, confidential, privileged, classified, commercial, proprietary or sensitive information, documents and plans, relating to the Project or its occupants or other matters, the unauthorized disclosure of which could result in significant public safety, financial and other damage to the Port Authority, the Project, its occupants, and the surrounding communities; and

WHEREAS, Recipient recognizes and acknowledges that providing unauthorized access to, or disclosing such information to third parties in violation of the terms of this Agreement could compromise or undermine the existing or future guidelines, techniques and procedures implemented for the protection against terrorist acts or for law enforcement, investigation and

prosecutorial purposes, and accordingly could result in significant irreparable harm and injury; and

WHEREAS, in order to protect and preserve the privilege attaching to and the confidentiality of the aforementioned information as well as to limit access to such information to a strict need to know basis, the Port Authority requires, as a condition of its sharing or providing access to such protected, confidential, privileged, classified, commercial, proprietary or sensitive information, documents and plans, that the Recipient enter into this Agreement and that its Related Parties thereafter acknowledge and agree that they will be required to treat as strictly confidential and/or privileged any of such information so provided, as well as the work product and conclusions of any assessments and evaluations or any recommendations relating thereto, and to also fully comply with applicable federal rules and regulations with respect thereto; and

WHEREAS, as a condition to the provision of such information to Recipient and certain Related Parties, the Recipient has agreed to enter into this Agreement with respect to the handling and use of such information and to cause Related Parties to join in and be bound by the terms and conditions of this Agreement.

NOW, THEREFORE, in consideration of the provision by Port Authority of Information for Project Purposes (as each such term is defined below) and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged by the Recipient and each Related Party that receives such Information, the Recipient and each such Related Party agrees, as follows:

1. **Defined Terms**. In addition to the terms defined in the Recitals above, the following terms shall have the meanings set forth below:

(a) **"Authorized Disclosure**" means the disclosure of Protected Information strictly in accordance with the Confidentiality Control Procedures applicable thereto: (i) as to all Protected Information, only to a Related Party that has a need to know such Protected Information strictly for Project Purposes and that has agreed in writing to be bound by the terms of this Agreement by executing a form of Acknowledgment as set forth in Exhibit A or Exhibit B, as applicable; and (ii) as to Confidential Privileged Information, only to the extent expressly approved in writing and in advance by the Port Authority, and then only the particular Confidential Privileged Information that is required to accomplish an essential element of the Project.

(b) "**Information**" means, collectively, all information, documents, data, reports, notes, studies, projections, records, manuals, graphs, electronic files, computer generated data or information, drawings, charts, tables, diagrams, photographs, and other media or renderings containing or otherwise incorporating information that may be provided or made accessible at any time, whether in writing, orally, visually, photographically, electronically or in any other form or medium, including, without limitation, any and all copies, duplicates or extracts of the foregoing.

(c) "**Protected Information**" means and includes collectively, Confidential Information, Confidential Privileged Information, Sensitive Security Information (SSI), Critical Infrastructure Information (CII) or Health Insurance Portability and Accountability Act (HIPPA) Information and Information that is labeled, marked or otherwise identified by or on behalf of the Port Authority so as to reasonably connote that such information is confidential, privileged, sensitive or proprietary in nature. The term Protected Information shall also include all work product that contains or is derived from any of the foregoing, whether in whole or in part, regardless of whether prepared by the Recipient, the Port Authority or others, or when the Port Authority receives such information from others and agrees to treat such information as Protected. The following Information shall not constitute Protected Information for the purpose of this Agreement:

(i) Particular Information, other than Confidential Privileged Information, that is provided to the Recipient by a source other than the Port Authority, provided that such source is not subject to a confidentiality agreement, or similar obligation, or understanding with or for the benefit of the Port Authority, with respect to such Information and that the identity of such source is not itself part of such Protected Information.

(ii) Information that is or becomes generally available to the public other than as a result of a disclosure by the Recipient or a Related Party in violation of this Agreement.

(iii) Information that is known to or was in the possession of the Recipient or a Related Party on a non-confidential basis prior to the disclosure of such Information by the Port Authority.

(d) "**Confidential Information**" means and includes collectively, any and all Information, documents and materials entitled to protection as a public interest privilege under New York State law and as may be deemed to be afforded or entitled to the protection of any other privilege recognized under New York and/or New Jersey state laws or Federal laws. It also includes information that contains sensitive financial, commercial or other proprietary business information concerning or relating to the Port Authority, its projects, operations or facilities that would be exempt from release under the Port Authority Freedom of Information Code.

(e) "**Confidential Privileged Information**" means and includes collectively, (i) Information that reveals security risks, threats, vulnerabilities, documentation that identifies specific physical security vulnerabilities or revealing specific security vulnerabilities details related to emergency response protocols, egress plans, flow paths, egress capacities, (diagrams, codes, standards) etc., which is not publicly available." and any and all Information, documents and materials entitled to protection as a public interest privilege under New York State law and as may be deemed to be afforded or entitled to the protection of any other privilege recognized under New York and/or New Jersey state laws or Federal laws, and (ii) certain Critical Infrastructure Information.

(f) "**Confidentiality Control Procedures**" means procedures, safeguards and requirements for the identification, processing, protection, handling, care, tracking and storage of

Protected Information that are required under applicable federal or state law, the Port Authority Handbook, or by the terms of this Agreement.

(g) "**Critical Infrastructure Information**" (CII) has the meaning set forth in the Homeland Security Act of 2002, under the subtitle Critical Infrastructure Information Act of 2002 (6 U.S.C. §131-134), and any rules or regulations enacted pursuant thereto, including, without limitation, the Office of the Secretary, Department of Homeland Security Rules and Regulations, 6 C.F.R. Part 29 and any amendments thereto. CII may also be referred to as "Protected Critical Infrastructure Information" or "PCII", as provided for in the referenced rules and regulations and any amendments thereto.

(h) "**Sensitive Security Information**" (SSI) has the definition and requirements set forth in the Transportation Security Administrative Rules & Regulations, 49 CFR 1520, (49 U.S.C. §114) and in the Office of the Secretary of Transportation Rules & Regulations, 49 CFR 15, (49 U.S.C. §40119).

(i) "**Health Insurance Portability and Accountability Act**" (HIPAA) Information Employees, associates or other contract personnel who have access to Protected Health Information (PHI) must refer to, and comply with, the Privacy Policies and Procedures to Protect Personal Health Information. Privacy regulations issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA" or "Privacy Laws") place restrictions on the Group Health Plans of the Port Authority and PATH (the "Plans") ability to use and disclose Protected Health Information ("PHI").

(j) "**Port Authority Handbook**" means The Port Authority of New York and New Jersey. Information Security Handbook, as may be amended by the Port Authority, from time to time.

(k) **"Project Purposes**" means the use of Protected Information strictly and only for purposes related to Recipient's and its Related Parties' participation and involvement in the Project, and only for such period of time during which Recipient and its Related Parties are involved in Project related activities.

(l) "**Related Party**" and "**Related Parties**" means the directors, employees, officers, partners or members of the Recipient, as applicable, and the Recipient's outside consultants, attorneys, advisors, accountants, architects, engineers or subcontractors or sub-consultants (and their respective directors, employees, officers, partners or members) to whom any Protected Information is disclosed or made available.

2. **Use of Protected Information**. All Protected Information shall be used by the Recipient in accordance with the following requirements:

(a) All Protected Information shall be held in confidence and shall be processed, treated, disclosed and used by the Recipient and its Related Parties only for Project Purposes and in accordance with the Confidentiality Control Procedures established pursuant to Paragraph 2(c), below, including, without limitation, the Port Authority Handbook, receipt of which is acknowledged by Recipient and shall be acknowledged in writing by each Related Party by signing the Acknowledgment attached hereto as Exhibit A or Exhibit B, as applicable, and

applicable legal requirements. Protected Information may be disclosed, only if and to the extent that such disclosure is an Authorized Disclosure.

(b) Recipient and each Related Party acknowledges and agrees that (i) any violation by the Recipient or any of its Related Parties of the terms, conditions or restrictions of this Agreement relating to Protected Information may result in penalties and other enforcement or corrective action as set forth in such statutes and regulations, including, without limitation, the issuance of orders requiring retrieval of Sensitive Security Information and Critical Infrastructure Information to remedy unauthorized disclosure and to cease future unauthorized disclosure and (ii) pursuant to the aforementioned Federal Regulations, including, without limitation, 49 C.F.R. §§ 15.17 and 1520.17, any such violation thereof or mishandling of information therein defined may constitute grounds for a civil penalty and other enforcement or corrective action by the United States Department of Transportation and the United States Department of Homeland Security, and appropriate personnel actions for Federal employees.

(c) Recipient and each Related Party covenants to the Port Authority that it has established, promulgated and implemented Confidentiality Control Procedures for identification, handling, receipt, care, and storage of Protected Information to control and safeguard against any violation of the requirements of this Agreement and against any unauthorized access, disclosure, modification, loss or misuse of Protected Information. Recipient and each Related Party shall undertake reasonable steps consistent with such Confidentiality Control Procedures to assure that disclosure of Protected Information is compartmentalized, such that all Protected Information shall be disclosed only to those persons and entities authorized to receive such Information as an Authorized Disclosure under this Agreement and applicable Confidentiality Control Procedures. The Confidentiality Control Procedures shall, at a minimum, adhere to, and shall not be inconsistent with, the procedures and practices established in the Port Authority Handbook.

(d) The Port Authority reserves the right to audit Recipient's Confidentiality Control Procedures, and those of each Related Party, as applicable, to ensure that it is in compliance with the terms of this Agreement.

(e) The Port Authority may request in writing that the Recipient or any Related Parties apply different or more stringent controls on the handling, care, storage and disclosure of particular items of Protected Information as a precondition for its disclosure. The Port Authority may decline any request by the Recipient or any of its Related Parties to provide such item of Protected Information if the Recipient or any of the Related Parties do not agree in writing to apply such controls.

(f) Nothing in this Agreement shall require the Port Authority to tender or provide access to or possession of any Protected Information to the Recipient or its Related Parties, whether or not the requirements of this Agreement are otherwise satisfied. However, if such Protected Information is provided and accepted, the Recipient and its Related Parties shall abide by the terms, conditions and requirements of this Agreement.

(g) The Recipient and each Related Party agrees to be responsible for enforcing the provisions of this Agreement with respect to its Related Parties, in accordance with the Confidentiality Control Procedures. Except as required by law pursuant to written advice of

competent legal counsel, or with the Port Authority's prior written consent, neither the Recipient, nor any of the Related Parties shall disclose to any third party, person or entity: (i) any Protected Information under circumstances where the Recipient is not fully satisfied that the person or entity to whom such disclosure is about to be made shall act in accordance with the Confidentiality Control Procedures whether or not such person or entity has agreed in writing to be bound by the terms of this Agreement or any "Acknowledgement" of its terms or (ii) the fact that Protected Information has been made available to the Recipient or such Related Parties, or the content or import of such Protected Information. The Recipient is responsible for collecting and managing the Acknowledgments signed by Related Parties pursuant to this Agreement. Recipient shall, at the Port Authority's request, provide the Port Authority a list of all Related Parties who have signed an Acknowledgment, and copies of such Acknowledgments.

(h) As to all Protected Information provided by or on behalf of the Port Authority, nothing in this Agreement shall constitute or be construed as a waiver of any public interest privilege or other protections established under applicable state or federal law.

3. **Disclosures and Discovery Requests**. If a subpoena, discovery request, Court Order, Freedom of Information Request, or any other request or demand authorized by law seeking disclosure of the Protected Information is received by the Recipient or any Related Party, Recipient shall notify the Port Authority thereof, to the extent permitted by law, with sufficient promptness so as to enable the Port Authority to investigate the circumstances, prepare any appropriate documentation and seek to quash the subpoena, to seek a protective order, or to take such other action regarding the request as it deems appropriate. In the absence of a protective order, disclosure shall be made, in consultation with the Port Authority, of only that part of the Protected Information as is legally required to be disclosed. If at any time Protected Information is disclosed in violation of this Agreement, the Recipient shall immediately give the Port Authority written notice of that fact and a detailed account of the circumstances regarding such disclosure to the Port Authority.

4. **Retention Limitations; Return of Protected Information**. Upon the earlier occurrence of either the Port Authority's written request or completion of Recipient's need for any or all Protected Information, such Protected Information, all writings and material describing, analyzing or containing any part of such Protected Information, including any and all portions of Protected Information that may be stored, depicted or contained in electronic or other media and all copies of the foregoing shall be promptly delivered to the Port Authority at Recipient's expense. In addition, as to Protected Information that may be stored in electronic or similar form, such Protected Information shall be deleted and completely removed so that such Protected Information is incapable of being recovered from all computer databases of the Recipient and all Related Parties. The Recipient may request in writing that the Port Authority consent to destruction of Protected Information, writings and materials in lieu of delivery thereof to the Port Authority. The Port Authority shall not unreasonably withhold its consent to such request. If the Port Authority consents to such destruction, the Recipient and each Related Party shall deliver to the Port Authority a written certification by Recipient and such Related Party that such Protected Information, writings and materials have been so destroyed within such period as may be imposed by the Port Authority. Notwithstanding the foregoing, to the extent required for legal or compliance purposes, the Recipient may retain copies of Protected Information (in any format), provided that (a) the Port Authority is notified in writing of such retention, and (b) Recipient

continues to abide by the requirements of this Agreement with respect to the protection of such Protected Information.

5. **Duration and Survival of Confidentiality Obligations**. The obligations under this Agreement shall be perpetual (unless otherwise provided in this Agreement) or until such time as the Protected Information is no longer considered protected, confidential and/or privileged by the Port Authority.

6. **Severability**. Each provision of this Agreement is severable and if a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

7. **Injunctive and Other Relief**. Recipient and each Related Party acknowledges that the unauthorized disclosure and handling of Protected Information is likely to have a material adverse and detrimental impact on public safety and security and could significantly endanger the Port Authority, its facilities (including, without limitation, the Project site), its patrons and the general public and that damages at law are an inadequate remedy for any breach, or threatened breach, of this Agreement by Recipient or its Related Parties. The Port Authority shall be entitled, in addition to all other rights or remedies, to seek such restraining orders and injunctions as it may deem appropriate for any breach of this Agreement, without being required to show any actual damage or to post any bond or other security.

8. **Governing Law**. This Agreement shall be governed by and construed in accordance with the laws of the State of New York, without regard to conflict of laws principles. The Port Authority (subject to the terms of the Port Authority Legislation (as defined below)) and the Recipient specifically and irrevocably consent to the exclusive jurisdiction of any federal or state court in the County of New York and State of New York with respect to all matters concerning this Agreement and its enforcement. The Port Authority (subject to the terms of the Port Authority Legislation (as defined below)) and the Recipient agree that the execution and performance of this Agreement shall have a New York situs and, accordingly, they each consent (and solely with respect to the Port Authority, subject to the terms of the Port Authority Legislation (as defined below)) to personal jurisdiction in the State of New York for all purposes and proceedings arising from this Agreement. "**Port Authority Legislation**" shall mean the concurrent legislation of the State of New York and State of New Jersey set forth at Chapter 301 of the Laws of New York of 1950, as amended by Chapter 938 of the Laws of New York of 1974 (McKinney's Unconsolidated Laws §§7101-7112) and Chapter 204 of the Laws of New Jersey of 1951 (N.J.S.A. 32:1-157 to 32:1-168).

9. **Notices**. Any notice, demand or other communication (each, a "**notice**") that is given or rendered pursuant to this Agreement by either party to the other party, shall be: (i) given or rendered, in writing, (ii) addressed to the other party at its required address(es) for notices delivered to it as set forth below, and (iii) delivered by either (x) hand delivery, or (y) nationally recognized courier service (e.g., Federal Express, Express Mail). Any such notice shall be deemed given or rendered, and effective for purposes of this Agreement, as of the date actually delivered to the other party at such address(es) (whether or not the same is then received by other party due to a change of address of which no notice was given, or any rejection or refusal to accept delivery). Notices from either party (to the other) may be given by its counsel.

The required address(es) of each party for notices delivered to it is (are) as set forth below. Each party, however, may, from time to time, designate an additional or substitute required address(es) for notices delivered to it, provided that such designation must be made by notice given in accordance with this Paragraph 9.

Original to the Port Authority:	[8a]
	The Port Authority of New York and New Jersey
	[8b]
	[8c]
with a copy to:	The Port Authority of New York and New Jersey
	4 World Trade Center
	150 Greenwich Street, 24th Floor
	New York, NY 10007
	Attn: General Counsel's Office c/o Caroline Ioannou, Law DISO

If to the Recipient: _____

_____

_____

with a copy to: _____

_____

_____

10. **Entire Agreement**. This Agreement contains the complete statement of all the agreements among the parties hereto with respect to the subject matter thereof, and all prior agreements among the parties hereto respecting the subject matter hereof, whether written or oral, are merged herein and shall be of no further force or effect. This Agreement may not be changed, modified, discharged, or terminated, except by an instrument in writing signed by all of the parties hereto.

11. **Counterparts**. This Agreement may be executed in one or more counterparts, each of which shall be deemed to be an original, but all of which shall be one and the same document.

12. **Parties Bound**. This Agreement shall be binding upon the Recipient and its respective successors. The foregoing shall not be affected by the failure of any Related Party to join in this Agreement or to execute and deliver an Acknowledgement hereof.

13. **Authority**. The undersigned individual(s) executing this Agreement on behalf of the Recipient below represent(s) that they are authorized to execute this Agreement on behalf of the Recipient and to legally bind such party.

14. **Disclosure of Ownership Rights or License**. Nothing contained herein shall be construed as the granting or conferring by the Port Authority of any rights by ownership, license or otherwise in any Information.

15. **No Liability**. Neither the Commissioners of the Port Authority, nor any of them, nor any officer, agent or employee thereof, shall be charged personally by the Recipient with any liability, or held liable to the Recipient under any term or provision of this Agreement, or

because of its execution or attempted execution or because of any breach, or attempted or alleged breach thereof.

16. **Construction**. This Agreement is the joint product of the parties hereto and each provision of this Agreement has been subject to the mutual consultation, negotiation, and agreement of the parties hereto, and shall not be construed for or against any party hereto. The captions of the various sections in this Agreement are for convenience only and do not, and shall not be deemed to, define, limit or construe the contents of such Sections.

RECIPIENT:

Signature: _____

Print Name: [9]

Title: [10]

Date: [11]

EXHIBIT A

ACKNOWLEDGMENT BY RELATED PARTY INDIVIDUAL

I, [1] ("**Related Party**"), am employed as a(n) [2] by [3]. I have been provided with and have read the Non Disclosure and Confidentiality Agreement between [4] (the "**Recipient**") and The Port Authority of New York and New Jersey (the "**Port Authority**") dated [5a] [5b], [5c] (hereinafter the "**Agreement**"), and the Port Authority Handbook attached to the Agreement. I understand that because of my employer's relationship with [6], both my employer and I may be provided with access to, and/or copies of, sensitive security materials, protected or confidential information. If it is required for me to review or receive Protected Information, as it is defined in the aforementioned Agreement, I acknowledge that I will be bound by each and every term and provision contained therein, and that failure to do so may include, but is not limited to, the imposition of disciplinary action and sanctions, and/or the institution of legal action seeking injunctive relief, monetary and/or criminal penalties for violation of law and/or Port Authority policies and procedures, as well as for violation of federal and/or state regulations.

To the extent that I am currently in the possession of, or have previously come into contact with, marked information as it relates to the aforementioned Agreement, I agree to conform my handling procedures for Protected Information to the practices and procedures set forth and defined herein, or risk loss of access to said Information, removal from said Project and/or subjecting myself to the aforementioned disciplinary actions and/or civil and criminal penalties.

Signature: _____

Print Name: [7]

Date: [8]

EXHIBIT B

ACKNOWLEDGMENT BY RELATED PARTY ENTITY

The undersigned, [1], is the [2] of [3], a [4] ("**Related Party**"), located at [5], and is duly authorized to execute this Acknowledgment on behalf of the above Related Party. The above Related Party is involved with the functions of [6] in connection with [7] for The Port Authority of New York and New Jersey (the "**Port Authority**"). I acknowledge and confirm that the above named Related Party has been provided with a copy of and shall be bound and shall abide by all of the terms, requirements and conditions set forth in the Non Disclosure and Confidentiality Agreement dated [8a] [8b], [8c], between [9] (the "**Recipient**") and the Port Authority (hereinafter the "**Agreement**"), and by the Port Authority Handbook described in the Agreement. Appropriate and responsible officers and employees of the Related Party have carefully read and understand the terms and conditions of the Agreement. The Related Party has notice and acknowledges that any breach or violation of such terms, requirements and conditions may result in the imposition of remedies or sanctions as set forth or otherwise described therein against such Related Party.

Signature: _____

Print Name: [10]

Date: [11]

B-2
Non-Disclosure and Confidentiality Agreement without reference to Handbook

NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT
BETWEEN

[1]

AND

THE PORT AUTHORITY OF NEW YORK AND NEW JERSEY

THIS NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT (this "**Agreement**") is made as of this [2] day of [3], [4], by and between **THE PORT AUTHORITY OF NEW YORK AND NEW JERSEY** (the "**Port Authority**") a body corporate and politic created by Compact between the States of New York and New Jersey, with the consent of the Congress of the United States, and having an office and place of business at 4 World Trade Center, 150 Greenwich Street, New York, New York, 10007, and [5] having an office and place of business at [6] ("**Recipient**").

WHEREAS, the Port Authority desires, subject to the terms and conditions set forth below, to disclose to Recipient Protected Information (as defined below) in connection with [7] (collectively, the "Project(s)", or "Proposed Project(s)"); and

WHEREAS, the Recipient acknowledges that the Port Authority, in furtherance of its performance of essential and critical governmental functions relating to the Project, has existing and significant interests and obligations in establishing, maintaining and protecting the security and safety of the Project site and surrounding areas and related public welfare matters; and

WHEREAS, in furtherance of critical governmental interests regarding public welfare, safety and security at the Project site, the Port Authority has collected information and undertaken the development of certain plans and recommendations regarding the security, safety and protection of the Project site, including the physical construction and current and future operations; and

WHEREAS, the Port Authority and Recipient (collectively, the "**Parties**") acknowledge that in order for Recipient to undertake its duties and/or obligations with regard to its involvement in the Project, the Port Authority may provide Recipient or certain of its Related Parties (as defined below) certain information in the possession of the Port Authority, which may contain or include protected, confidential, privileged, classified, commercial, proprietary or sensitive information, documents and plans, relating to the Project or its occupants or other matters, the unauthorized disclosure of which could result in significant public safety, financial and other damage to the Port Authority, the Project, its occupants, and the surrounding communities; and

WHEREAS, Recipient recognizes and acknowledges that providing unauthorized access to, or disclosing such information to third parties in violation of the terms of this Agreement could compromise or undermine the existing or future guidelines, techniques and procedures implemented for the protection against terrorist acts or for law enforcement, investigation and prosecutorial purposes, and accordingly could result in significant irreparable harm and injury; and

WHEREAS, in order to protect and preserve the privilege attaching to and the confidentiality of the aforementioned information as well as to limit access to such information to a strict need to know basis, the Port Authority requires, as a condition of its sharing or providing access to such protected, confidential, privileged, classified, commercial, proprietary or sensitive information, documents and plans, that the Recipient enter into this Agreement and that its Related Parties thereafter acknowledge and agree that they will be required to treat as strictly confidential and/or privileged any of such information so provided, as well as the work product and conclusions of any assessments and evaluations or any recommendations relating thereto, and to also fully comply with applicable federal rules and regulations with respect thereto; and

WHEREAS, as a condition to the provision of such information to Recipient and certain Related Parties, the Recipient has agreed to enter into this Agreement with respect to the handling and use of such information and to cause Related Parties to join in and be bound by the terms and conditions of this Agreement.

NOW, THEREFORE, in consideration of the provision by Port Authority of Information for Project Purposes (as each such term is defined below) and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged by the Recipient and each Related Party that receives such Information, the Recipient and each such Related Party agrees, as follows:

17. **Defined Terms**. In addition to the terms defined in the Recitals above, the following terms shall have the meanings set forth below:

(a) **"Authorized Disclosure**" means the disclosure of Protected Information strictly in accordance with the Confidentiality Control Procedures applicable thereto: (i) as to all Protected Information, only to a Related Party that has a need to know such Protected Information strictly for Project Purposes and that has agreed in writing to be bound by the terms of this Agreement by executing a form of Acknowledgment as set forth in Exhibit A or Exhibit B, as applicable; and (ii) as to Confidential Privileged Information, only to the extent expressly approved in writing and in advance by the Port Authority, and then only the particular Confidential Privileged Information that is required to accomplish an essential element of the Project.

(b) "**Information**" means, collectively, all information, documents, data, reports, notes, studies, projections, records, manuals, graphs, electronic files, computer generated data or information, drawings, charts, tables, diagrams, photographs, and other media or renderings containing or otherwise incorporating information that may be provided or made accessible at any time, whether in writing, orally, visually, photographically, electronically or in any other

form or medium, including, without limitation, any and all copies, duplicates or extracts of the foregoing.

(c) "**Protected Information**" means and includes collectively, Confidential Information, Confidential Privileged Information, Sensitive Security Information (SSI), Critical Infrastructure Information (CII) or Health Insurance Portability and Accountability Act (HIPPA) Information and Information that is labeled, marked or otherwise identified by or on behalf of the Port Authority so as to reasonably connote that such information is confidential, privileged, sensitive or proprietary in nature. The term Protected Information shall also include all work product that contains or is derived from any of the foregoing, whether in whole or in part, regardless of whether prepared by the Recipient, the Port Authority or others, or when the Port Authority receives such information from others and agrees to treat such information as Protected. The following Information shall not constitute Protected Information for the purpose of this Agreement:

(i) Particular Information, other than Confidential Privileged Information, that is provided to the Recipient by a source other than the Port Authority, provided that such source is not subject to a confidentiality agreement, or similar obligation, or understanding with or for the benefit of the Port Authority, with respect to such Information and that the identity of such source is not itself part of such Protected Information.

(ii) Information that is or becomes generally available to the public other than as a result of a disclosure by the Recipient or a Related Party in violation of this Agreement.

(iii) Information that is known to or was in the possession of the Recipient or a Related Party on a non-confidential basis prior to the disclosure of such Information by the Port Authority.

(d) "**Confidential Information**" means and includes collectively, any and all Information, documents and materials entitled to protection as a public interest privilege under New York State law and as may be deemed to be afforded or entitled to the protection of any other privilege recognized under New York and/or New Jersey state laws or Federal laws. It also includes information that contains sensitive financial, commercial or other proprietary business information concerning or relating to the Port Authority, its projects, operations or facilities that would be exempt from release under the Port Authority Freedom of Information Code.

(e) "**Confidential Privileged Information**" means and includes collectively, (i) Information that reveals security risks, threats, vulnerabilities, documentation that identifies specific physical security vulnerabilities or revealing specific security vulnerabilities details related to emergency response protocols, egress plans, flow paths, egress capacities, (diagrams, codes, standards) etc., which is not publicly available." and any and all Information, documents and materials entitled to protection as a public interest privilege under New York State law and as may be deemed to be afforded or entitled to the protection of any other privilege recognized under New York and/or New Jersey state laws or Federal laws, and (ii) certain Critical Infrastructure Information.

(f) "**Confidentiality Control Procedures**" means procedures, safeguards and requirements for the identification, processing, protection, handling, care, tracking and storage of Protected Information that are required under applicable federal or state law or by the terms of this Agreement.

(g) "**Critical Infrastructure Information**" (CII) has the meaning set forth in the Homeland Security Act of 2002, under the subtitle Critical Infrastructure Information Act of 2002 (6 U.S.C. §131-134), and any rules or regulations enacted pursuant thereto, including, without limitation, the Office of the Secretary, Department of Homeland Security Rules and Regulations, 6 C.F.R. Part 29 and any amendments thereto. CII may also be referred to as "Protected Critical Infrastructure Information" or "PCII", as provided for in the referenced rules and regulations and any amendments thereto.

(h) "**Sensitive Security Information**" (SSI) has the definition and requirements set forth in the Transportation Security Administrative Rules & Regulations, 49 CFR 1520, (49 U.S.C. §114) and in the Office of the Secretary of Transportation Rules & Regulations, 49 CFR 15, (49 U.S.C. §40119).

(i) "**Health Insurance Portability and Accountability Act**" (HIPAA) Information Employees, associates or other contract personnel who have access to Protected Health Information (PHI) must refer to, and comply with, the Privacy Policies and Procedures to Protect Personal Health Information. Privacy regulations issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA" or "Privacy Laws") place restrictions on the Group Health Plans of the Port Authority and PATH (the "Plans") ability to use and disclose Protected Health Information ("PHI").

(j) **"Project Purposes**" means the use of Protected Information strictly and only for purposes related to Recipient's and its Related Parties' participation and involvement in the Project, and only for such period of time during which Recipient and its Related Parties are involved in Project related activities.

(k) "**Related Party**" and "**Related Parties**" means the directors, employees, officers, partners or members of the Recipient, as applicable, and the Recipient's outside consultants, attorneys, advisors, accountants, architects, engineers or subcontractors or sub-consultants (and their respective directors, employees, officers, partners or members) to whom any Protected Information is disclosed or made available.

18. **Use of Protected Information**. All Protected Information shall be used by the Recipient in accordance with the following requirements:

(a) All Protected Information shall be held in confidence and shall be processed, treated, disclosed and used by the Recipient and its Related Parties only for Project Purposes and in accordance with the Confidentiality Control Procedures established pursuant to Paragraph 2(c), below, and applicable legal requirements. Protected Information may be disclosed, only if and to the extent that such disclosure is an Authorized Disclosure.

(b) Recipient and each Related Party acknowledges and agrees that (i) any violation by the Recipient or any of its Related Parties of the terms, conditions or restrictions of this

Agreement relating to Protected Information may result in penalties and other enforcement or corrective action as set forth in such statutes and regulations, including, without limitation, the issuance of orders requiring retrieval of Sensitive Security Information and Critical Infrastructure Information to remedy unauthorized disclosure and to cease future unauthorized disclosure and (ii) pursuant to the aforementioned Federal Regulations, including, without limitation, 49 C.F.R. §§ 15.17 and 1520.17, any such violation thereof or mishandling of information therein defined may constitute grounds for a civil penalty and other enforcement or corrective action by the United States Department of Transportation and the United States Department of Homeland Security, and appropriate personnel actions for Federal employees.

(c) Recipient and each Related Party covenants to the Port Authority that it has established, promulgated and implemented Confidentiality Control Procedures for identification, handling, receipt, care, and storage of Protected Information to control and safeguard against any violation of the requirements of this Agreement and against any unauthorized access, disclosure, modification, loss or misuse of Protected Information. Recipient and each Related Party shall undertake reasonable steps consistent with such Confidentiality Control Procedures to assure that disclosure of Protected Information is compartmentalized, such that all Protected Information shall be disclosed only to those persons and entities authorized to receive such Information as an Authorized Disclosure under this Agreement and applicable Confidentiality Control Procedures. To assist Recipient in its determination of the adequacy of its Confidentiality Control Procedures, Recipient has been provided with a copy of the Port Authority's Information Security Handbook.

(d) The Port Authority reserves the right to audit Recipient's Confidentiality Control Procedures, and those of each Related Party, as applicable, to ensure that it is in compliance with the terms of this Agreement.

(e) The Port Authority may request in writing that the Recipient or any Related Parties apply different or more stringent controls on the handling, care, storage and disclosure of particular items of Protected Information as a precondition for its disclosure. The Port Authority may decline any request by the Recipient or any of its Related Parties to provide such item of Protected Information if the Recipient or any of the Related Parties do not agree in writing to apply such controls.

(f) Nothing in this Agreement shall require the Port Authority to tender or provide access to or possession of any Protected Information to the Recipient or its Related Parties, whether or not the requirements of this Agreement are otherwise satisfied. However, if such Protected Information is provided and accepted, the Recipient and its Related Parties shall abide by the terms, conditions and requirements of this Agreement.

(g) The Recipient and each Related Party agrees to be responsible for enforcing the provisions of this Agreement with respect to its Related Parties, in accordance with the Confidentiality Control Procedures. Except as required by law pursuant to written advice of competent legal counsel, or with the Port Authority's prior written consent, neither the Recipient, nor any of the Related Parties shall disclose to any third party, person or entity: (i) any Protected Information under circumstances where the Recipient is not fully satisfied that the person or entity to whom such disclosure is about to be made shall act in accordance with the

Confidentiality Control Procedures whether or not such person or entity has agreed in writing to be bound by the terms of this Agreement or any "Acknowledgement" of its terms or (ii) the fact that Protected Information has been made available to the Recipient or such Related Parties, or the content or import of such Protected Information. The Recipient is responsible for collecting and managing the Acknowledgments signed by Related Parties pursuant to this Agreement. Recipient shall, at the Port Authority's request, provide the Port Authority a list of all Related Parties who have signed an Acknowledgment, and copies of such Acknowledgments.

(h) As to all Protected Information provided by or on behalf of the Port Authority, nothing in this Agreement shall constitute or be construed as a waiver of any public interest privilege or other protections established under applicable state or federal law.

19. **Disclosures and Discovery Requests**. If a subpoena, discovery request, Court Order, Freedom of Information Request, or any other request or demand authorized by law seeking disclosure of the Protected Information is received by the Recipient or any Related Party, Recipient shall notify the Port Authority thereof, to the extent permitted by law, with sufficient promptness so as to enable the Port Authority to investigate the circumstances, prepare any appropriate documentation and seek to quash the subpoena, to seek a protective order, or to take such other action regarding the request as it deems appropriate. In the absence of a protective order, disclosure shall be made, in consultation with the Port Authority, of only that part of the Protected Information as is legally required to be disclosed. If at any time Protected Information is disclosed in violation of this Agreement, the Recipient shall immediately give the Port Authority written notice of that fact and a detailed account of the circumstances regarding such disclosure to the Port Authority.

20. **Retention Limitations; Return of Protected Information**. Upon the earlier occurrence of either the Port Authority's written request or completion of Recipient's need for any or all Protected Information, such Protected Information, all writings and material describing, analyzing or containing any part of such Protected Information, including any and all portions of Protected Information that may be stored, depicted or contained in electronic or other media and all copies of the foregoing shall be promptly delivered to the Port Authority at Recipient's expense. In addition, as to Protected Information that may be stored in electronic or similar form, such Protected Information shall be deleted and completely removed so that such Protected Information is incapable of being recovered from all computer databases of the Recipient and all Related Parties. The Recipient may request in writing that the Port Authority consent to destruction of Protected Information, writings and materials in lieu of delivery thereof to the Port Authority. The Port Authority shall not unreasonably withhold its consent to such request. If the Port Authority consents to such destruction, the Recipient and each Related Party shall deliver to the Port Authority a written certification by Recipient and such Related Party that such Protected Information, writings and materials have been so destroyed within such period as may be imposed by the Port Authority. Notwithstanding the foregoing, to the extent required for legal or compliance purposes, the Recipient may retain copies of Protected Information (in any format), provided that (a) the Port Authority is notified in writing of such retention, and (b) Recipient continues to abide by the requirements of this Agreement with respect to the protection of such Protected Information.

21. **Duration and Survival of Confidentiality Obligations**. The obligations under this Agreement shall be perpetual (unless otherwise provided in this Agreement) or until such time as the Protected Information is no longer considered protected, confidential and/or privileged by the Port Authority.

22. **Severability**. Each provision of this Agreement is severable and if a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

23. **Injunctive and Other Relief**. Recipient and each Related Party acknowledges that the unauthorized disclosure and handling of Protected Information is likely to have a material adverse and detrimental impact on public safety and security and could significantly endanger the Port Authority, its facilities (including, without limitation, the Project site), its patrons and the general public and that damages at law are an inadequate remedy for any breach, or threatened breach, of this Agreement by Recipient or its Related Parties. The Port Authority shall be entitled, in addition to all other rights or remedies, to seek such restraining orders and injunctions as it may deem appropriate for any breach of this Agreement, without being required to show any actual damage or to post any bond or other security.

24. **Governing Law**. This Agreement shall be governed by and construed in accordance with the laws of the State of New York, without regard to conflict of laws principles. The Port Authority (subject to the terms of the Port Authority Legislation (as defined below)) and the Recipient specifically and irrevocably consent to the exclusive jurisdiction of any federal or state court in the County of New York and State of New York with respect to all matters concerning this Agreement and its enforcement. The Port Authority (subject to the terms of the Port Authority Legislation (as defined below)) and the Recipient agree that the execution and performance of this Agreement shall have a New York situs and, accordingly, they each consent (and solely with respect to the Port Authority, subject to the terms of the Port Authority Legislation (as defined below)) to personal jurisdiction in the State of New York for all purposes and proceedings arising from this Agreement. "**Port Authority Legislation**" shall mean the concurrent legislation of the State of New York and State of New Jersey set forth at Chapter 301 of the Laws of New York of 1950, as amended by Chapter 938 of the Laws of New York of 1974 (McKinney's Unconsolidated Laws §§7101-7112) and Chapter 204 of the Laws of New Jersey of 1951 (N.J.S.A. 32:1-157 to 32:1-168).

25. **Notices**. Any notice, demand or other communication (each, a "**notice**") that is given or rendered pursuant to this Agreement by either party to the other party, shall be: (i) given or rendered, in writing, (ii) addressed to the other party at its required address(es) for notices delivered to it as set forth below, and (iii) delivered by either (x) hand delivery, or (y) nationally recognized courier service (e.g., Federal Express, Express Mail). Any such notice shall be deemed given or rendered, and effective for purposes of this Agreement, as of the date actually delivered to the other party at such address(es) (whether or not the same is then received by other party due to a change of address of which no notice was given, or any rejection or refusal to accept delivery). Notices from either party (to the other) may be given by its counsel.

The required address(es) of each party for notices delivered to it is (are) as set forth below. Each party, however, may, from time to time, designate an additional or substitute

required address(es) for notices delivered to it, provided that such designation must be made by notice given in accordance with this Paragraph 9.

Original to the Port Authority:	[8a] The Port Authority of New York and New Jersey [8b] [8c]
with a copy to:	The Port Authority of New York and New Jersey 4 World Trade Center 150 Greenwich Street, 24th Floor New York, NY 10007 Attn: General Counsel's Office c/o Caroline Ioannou, Law DISO

If to the Recipient: _____

_____

_____

with a copy to: _____

_____

_____

26. **Entire Agreement**. This Agreement contains the complete statement of all the agreements among the parties hereto with respect to the subject matter thereof, and all prior agreements among the parties hereto respecting the subject matter hereof, whether written or oral, are merged herein and shall be of no further force or effect. This Agreement may not be changed, modified, discharged, or terminated, except by an instrument in writing signed by all of the parties hereto.

27. **Counterparts**. This Agreement may be executed in one or more counterparts, each of which shall be deemed to be an original, but all of which shall be one and the same document.

28. **Parties Bound**. This Agreement shall be binding upon the Recipient and its respective successors. The foregoing shall not be affected by the failure of any Related Party to join in this Agreement or to execute and deliver an Acknowledgement hereof.

29. **Authority**. The undersigned individual(s) executing this Agreement on behalf of the Recipient below represent(s) that they are authorized to execute this Agreement on behalf of the Recipient and to legally bind such party.

30. **Disclosure of Ownership Rights or License**. Nothing contained herein shall be construed as the granting or conferring by the Port Authority of any rights by ownership, license or otherwise in any Information.

31. **No Liability**. Neither the Commissioners of the Port Authority, nor any of them, nor any officer, agent or employee thereof, shall be charged personally by the Recipient with any

liability, or held liable to the Recipient under any term or provision of this Agreement, or because of its execution or attempted execution or because of any breach, or attempted or alleged breach thereof.

32. **Construction**. This Agreement is the joint product of the parties hereto and each provision of this Agreement has been subject to the mutual consultation, negotiation, and agreement of the parties hereto, and shall not be construed for or against any party hereto. The captions of the various sections in this Agreement are for convenience only and do not, and shall not be deemed to, define, limit or construe the contents of such Sections.

RECIPIENT:

Signature: _____

Print Name: [9]

Title: [10]

Date: [11]

EXHIBIT A

ACKNOWLEDGMENT BY RELATED PARTY INDIVIDUAL

I, [1] ("**Related Party**"), am employed as a(n) [2] by [3]. I have been provided with and have read the Non Disclosure and Confidentiality Agreement between [4] (the "**Recipient**") and The Port Authority of New York and New Jersey (the "**Port Authority**") dated [5a] [5b], [5c] (hereinafter the "**Agreement**".) I understand that because of my employer's relationship with [6], both my employer and I may be provided with access to, and/or copies of, sensitive security materials, protected or confidential information. If it is required for me to review or receive Protected Information, as it is defined in the aforementioned Agreement, I acknowledge that I will be bound by each and every term and provision contained therein, and that failure to do so may include, but is not limited to, the imposition of disciplinary action and sanctions, and/or the institution of legal action seeking injunctive relief, monetary and/or criminal penalties for violation of law and/or Port Authority policies and procedures, as well as for violation of federal and/or state regulations.

To the extent that I am currently in the possession of, or have previously come into contact with, marked information as it relates to the aforementioned Agreement, I agree to conform my handling procedures for Protected Information to the practices and procedures set forth and defined herein, or risk loss of access to said Information, removal from said Project and/or subjecting myself to the aforementioned disciplinary actions and/or civil and criminal penalties.

Signature: _____

Print Name: [7]

Date: [8]

EXHIBIT B

ACKNOWLEDGMENT BY RELATED PARTY ENTITY

The undersigned, [1], is the [2] of [3], a [4] ("**Related Party**"), located at [5], and is duly authorized to execute this Acknowledgment on behalf of the above Related Party. The above Related Party is involved with the functions of [6] in connection with [7] for The Port Authority of New York and New Jersey (the "**Port Authority**"). I acknowledge and confirm that the above named Related Party has been provided with a copy of and shall be bound and shall abide by all of the terms, requirements and conditions set forth in the Non Disclosure and Confidentiality Agreement dated [8a] [8b], [8c], between [9] (the "**Recipient**") and the Port Authority (hereinafter the "**Agreement**"). Appropriate and responsible officers and employees of the Related Party have carefully read and understand the terms and conditions of the Agreement. The Related Party has notice and acknowledges that any breach or violation of such terms, requirements and conditions may result in the imposition of remedies or sanctions as set forth or otherwise described therein against such Related Party.

Signature: _____

Print Name: [10]

Date: [11]

B-3
PA/PATH Non-Disclosure and Confidentiality Agreement

PA EMPLOYEE NON-DISCLOSURE
AND CONFIDENTIALITY AGREEMENT

THIS NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT (this "**Agreement**") is made as of this [1] day of [2], [3], by and between **THE PORT AUTHORITY OF NEW YORK AND NEW JERSEY,** a body corporate and politic created by Compact between the States of New York and New Jersey, with the consent of the Congress of the United States, and its related entities, including, but not limited to, Port Authority Trans-Hudson Corporation (collectively referred to as the "**Port Authority**") and having an office and place of business at 4 World Trade Center, 150 Greenwich Street, New York, New York, 10007, and [4], of [5] Department, an employee of the Port Authority ("**Employee**"), having the Port Authority Employee Number: [6].

WHEREAS, security is of critical importance to the Port Authority in carrying out its mission and in providing a safe and secure environment for its patrons and employees, as well as properly protecting its properties, facilities and operations; and

WHEREAS, the safeguarding of protected, confidential and sensitive information is an essential factor in the Port Authority's ability to carry out its responsibilities; and

WHEREAS, the Port Authority recognizes the need for providing its employees with access to certain information which may contain or include protected, confidential, privileged, classified, commercial, proprietary or sensitive information, documents and plans, on a need to know and/or an as-needed basis; and

WHEREAS, every employee having access to Protected Information (as hereinafter defined) has the obligation and the responsibility to properly safeguard such information and prevent its unauthorized disclosure or release.

NOW THEREFORE, Employee hereby agrees, as follows:

1. **Defined Terms.** In addition to the terms defined in the Recitals above, the following terms shall have the meanings set forth below:

    a. "**Protected Information**" means and includes collectively, Confidential Information, Confidential Privileged Information, Critical Infrastructure Information (CII), Sensitive Security Information (SSI), or Health Insurance Portability and

Accountability Act (HIPPA) Information and Information that is labeled, marked or otherwise identified by or on behalf of the Port Authority so as to reasonably connote that such information is confidential, privileged, sensitive or proprietary in nature. The term Protected Information shall also include all work product that contains or is derived from any of the foregoing, whether in whole or in part, regardless of whether prepared by the Recipient, the Port Authority or others, or when the Port Authority receives such information from others and agrees to treat such information as Protected.

b. "**Confidential Information**" means and includes collectively, any and all Information, documents and materials entitled to protection as a public interest privilege under New York State law and as may be deemed to be afforded or entitled to the protection of any other privilege recognized under New York and/or New Jersey state laws or Federal laws. It also includes information that contains sensitive financial, commercial or other proprietary business information concerning or relating to the Port Authority, its projects, operations or facilities that would be exempt from release under the Port Authority Freedom of Information Code.

c. "**Confidential Privileged Information**" means and includes collectively, (i) Information that reveals security risks, threats, vulnerabilities, documentation that identifies specific physical security vulnerabilities or revealing specific security vulnerabilities details related to emergency response protocols, egress plans, flow paths, egress capacities, (diagrams, codes, standards) etc., which is not publicly available." and any and all Information, documents and materials entitled to protection as a public interest privilege under New York State law and as may be deemed to be afforded or entitled to the protection of any other privilege recognized under New York and/or New Jersey state laws or Federal laws, and (ii) certain Critical Infrastructure Information.

d. "**Information**" means, collectively, all information, documents, data, reports, notes, studies, projections, records, manuals, graphs, electronic files, computer generated data or information, drawings, charts, tables, diagrams, photographs, and other media or renderings containing or otherwise incorporating information that may be provided or made accessible at any time, whether in writing, orally, visually, photographically, electronically or in any other form or medium, including, without limitation, any and all copies, duplicates or extracts of the foregoing.

e. "**Critical Infrastructure Information**" (CII) has the meaning set forth in the Homeland Security Act of 2002, under the subtitle Critical Infrastructure Information Act of 2002 (6 U.S.C. §131-134), and any rules or regulations enacted pursuant thereto, including, without limitation, the Office of the Secretary, Department of Homeland Security Rules and Regulations, 6 C.F.R. Part 29 and any amendments thereto. CII may also be referred to as "Protected Critical Infrastructure Information" or "PCII", as provided for in the referenced rules and regulations.

f. "**Sensitive Security Information**" (SSI) has the definition and requirements set forth in the Transportation Security Administrative Rules & Regulations, 49 CFR 1520,

(49 U.S.C. §114) and in the Office of the Secretary of Transportation Rules & Regulations, 49 CFR 15, (49 U.S.C. §40119).

g. "**Health Insurance Portability and Accountability Act**" (HIPAA) Information Employees, associates or other contract personnel who have access to Protected Health Information (PHI) must refer to, and comply with, the Privacy Policies and Procedures to Protect Personal Health Information. Privacy regulations issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA" or "Privacy Laws") place restrictions on the Group Health Plans of the Port Authority and PATH (the "Plans") ability to use and disclose Protected Health Information ("PHI").

h. **"Port Authority Handbook**" means The Port Authority of New York and New Jersey Information Security Handbook, as may be amended by the Port Authority, from time to time.

2. **Compliance with the Port Authority Handbook.** All Protected Information is to be handled by the Employee with the utmost care and in a manner designed to prevent its disclosure to unauthorized third parties consistent with Port Authority security policy, practices and procedures, as set forth in the Port Authority Handbook. Employee must maintain and dispose of Protected Information in a manner consistent with this Agreement and in conformity with the Port Authority Handbook.

3. **Use of Protected Information.** Protected Information provided to or obtained by Employee may only be used in the performance of duly authorized activities relating to the Employee's job duties, and may not be used for any other purpose, unless expressly authorized by this Agreement, or as expressly directed in writing by the Port Authority.

4. **Disclosure of Information.** Until such time as the Information is no longer considered Protected by the Port Authority, and that fact is communicated to the Employee in writing, the Information must be held and treated in the strictest confidence and may not, except in accordance with Paragraph 5, below, be disclosed to any person who has not agreed to be bound by a Non-Disclosure and Confidentiality Agreement. When disclosure of such Information is permitted under these circumstances, it will only be provided to such individuals to the extent that it is necessary for that person to perform his/her duly authorized activities at or in connection with their job responsibilities and may only be provided on a need-to-know-basis. Copies of documents or materials in any form, format or medium, which contain disclosures of such Information, may only be made pursuant to the procedures established in the Port Authority Handbook.

5. **Disclosures and Discovery Requests**. If a subpoena, discovery request, Court Order, Freedom of Information Request, or any other request or demand authorized by law is received by the Employee seeking disclosure of Protected Information, the Employee must immediately notify his/her Supervisor and Departmental Information Security Officer in

order to permit the Port Authority to seek to quash the subpoena, seek a protective order, or take such other action regarding the request as it deems appropriate, and the Employee will fully cooperate in the Port Authority's efforts in this regard. If at any time Protected Information is disclosed in violation of this Agreement, the employee will immediately report that fact and the circumstances regarding such disclosure to his/her Supervisor and Departmental Information Security Officer.

6. **Unauthorized Disclosure and Disciplinary Actions.** The unauthorized disclosure or improper handling of Protected Information could have an adverse and detrimental impact on public safety and security and could significantly endanger the Port Authority, its operations, its facilities, its patrons and the general public. Because of this, the obligations of confidence required hereunder are extraordinary and unique, and are vital to the security and well being of the Port Authority. Any failure to comply with, or any violation of, this Agreement, may result in legal action and/or disciplinary action against Employee.

7. **Duration and Survival of Confidentiality Obligations.** The obligations under this Agreement shall be perpetual, or until such time as the Protected Information is no longer considered protected, confidential and/or privileged by the Port Authority, and that fact is communicated in writing to Employee.

EMPLOYEE:

Signature: _____

Print Name: [7]

Date: [8]

APPENDIX C

Background Screening Criteria

S.W.A.C.™
Secure Worker Access Consortium

CONTENTS:

- Background Screening Specifications
- High Access Level Criteria
- Medium Access Level Criteria
- Standard Access Level Criteria

Criminal History
Background Screening Specifications

Social Security Number — Positive Identity Verification (PIV)
Federal District Court Search (each district of residence and employment)*
National Criminal Search*
Statewide Criminal Check (each state of residence and employment)*
County Criminal Search (each county of residence and employment)*
Sexual Offender Search (each resident state)*
Alien Immigrant Search
Immigration Violation Check
Fake Identification Convictions
State Driving Record
Check for material false statement or omission on application form
National Terrorist Watch List Search (OFAC-SDN)

Note* Within ten (10), seven (7), or five (5) years preceding date of application as noted on the HIGH, MEDIUM, and STANDARD Level of Clearance forms.

Level of Clearance

HIGH Secure Access Control Areas
and CONFIDENTIAL PRIVILEGED INFORMATION

I. No convictions ever in your lifetime: an individual has a disqualifying criminal offense if the individual was convicted, or found not guilty by reason of insanity, in a civilian or military jurisdiction of any of the following criminal offenses:

(1) Terrorism—A crime listed in 18 U.S.C. Chapter 113B—or a State law that is comparable.
(2) Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. 1961, et. seq., or a State law that is comparable.
(3) A crime involving a severe transportation security incident.
(4) Making any threat, or maliciously conveying false information knowing the same to be false, concerning the deliverance, placement, or detonation of an explosive or other lethal device in or against a place of public use, a state or government facility, a public transportations system, or an infrastructure facility.
(5) Improper transportation of a hazardous material under 49 U.S.C. 5124, or a state law that is comparable;
(6) Murder.
(7) Espionage.
(8) Sedition.
(9) Treason.
(10) Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of, or dealing in an explosive or explosive device.
(11) Conspiracy or attempt to commit any of the criminal acts listed in paragraph I.

II. An individual has a disqualifying criminal offense if the individual was convicted, or found not guilty by reason of insanity, in a civilian or military jurisdiction, within the **past ten (10) years** from completion of sentence preceding the date of the application, of the following offenses:

(1) Forgery of certificates, false marking of aircraft, and other aircraft registration violation;
(2) Interference with air navigation;
(3) Aircraft piracy;
(4) Interference with flight crewmembers or flight attendants;
(5) Commission of certain crimes aboard aircraft in flight;
(6) Carrying a weapon or explosive aboard aircraft;
(7) Conveying false information and threats; (e.g., bomb threats, explosives in briefcase, etc. in security areas)
(8) Aircraft piracy outside the special aircraft jurisdiction of the United States;
(9) Lighting violations involving transporting controlled substances;
(10) Unlawful entry into an aircraft or airport area that serves air carriers or foreign air carriers contrary to established security requirements;
(11) Destruction of an aircraft or aircraft facility;
(12) Assault with intent to murder.
(13) Kidnapping or hostage taking.
(14) Rape or aggravated sexual abuse.
(15) Extortion.
(16) Armed or felony unarmed robbery.

(17) Distribution of, possession with intent to distribute, or importation of a controlled substance.
(18) Felony arson.
(19) Felony involving a threat.
(20) Felony involving—
- (i) Willful destruction of property;
- (ii) Importation or manufacture of a controlled substance;
- (iii) Burglary or Robbery
- (iv) Theft;
- (v) Dishonesty, fraud, or misrepresentation, including identity fraud and money laundering;
- (vi) Possession or distribution of stolen property;
- (vii) Aggravated assault;
- (viii) Bribery; or
- (ix) Illegal possession of a controlled substance punishable by a maximum term of imprisonment of more than 1 year;
- (x) Smuggling;
- (xi) Immigration violations; or

(21) Violence at international airports;
(22) Unlawful possession, use, sale, manufacture, purchase, distribution, receipt, transfer, shipping, transporting, delivery, import, export of, or dealing in a firearm or other weapon. A firearm or other weapon includes, but is not limited to, firearms as defined in 18 U.S.C. 921(a)(3) or 26 U.S.C.5 845(a), or items contained on the U.S. Munitions Import List at 27 CFR 447.21.
(23) Conspiracy or attempt to commit any of the criminal acts listed in paragraph II.

Under want, warrant, or indictment. An applicant who is wanted, or under indictment in any civilian or military jurisdiction for a felony listed in section II, is disqualified until the want or warrant is released or the indictment is dismissed.

Level of Clearance

Up To MEDIUM Secure Access Control Areas and CONFIDENTIAL INFORMATION

I. No convictions ever in your lifetime: an individual has a disqualifying criminal offense if the individual was convicted, or found not guilty by reason of insanity, in a civilian or military jurisdiction of any of the following criminal offenses:

(1) Terrorism—A crime listed in 18 U.S.C. Chapter 113B—or a State law that is comparable.

(2) Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. 1961, et. seq., or a State law that is comparable.

(3) A crime involving a severe transportation security incident.

(4) Making any threat, or maliciously conveying false information knowing the same to be false, concerning the deliverance, placement, or detonation of an explosive or other lethal device in or against a place of public use, a state or government facility, a public transportations system, or an infrastructure facility. (3) Improper transportation of a hazardous material under 49 U.S.C. 5124, or a state law that is comparable;

(5) Improper transportation of a hazardous material under 49 U.S.C. 5124, or a state law that is comparable;

(6) Murder.

(7) Espionage.

(8) Sedition.

(9) Treason.

(10) Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of, or dealing in an explosive or explosive device.

(11) Conspiracy or attempt to commit any of the criminal acts listed in paragraph I.

II. An individual has a disqualifying criminal offense if the individual was convicted, or found not guilty by reason of insanity, in a civilian or military jurisdiction for the following offenses, within the **past ten (10) years** from completion of sentence for the offense preceding the date of the application:

(1) Extortion.

(2) Armed or felony unarmed robbery.

(3) Felony involving—

(i) Importation or manufacture of a controlled substance;

(ii) Burglary or Robbery;

(iii) Theft;

(iv) Dishonesty, fraud, or misrepresentation, including identity fraud and money laundering;

(v) Possession or distribution of stolen property;

(vi) Bribery; or

(4) Conspiracy or attempt to commit any of the criminal acts listed in paragraph II.

Under want, warrant, or indictment. An applicant who is wanted, or under indictment in any

civilian or military jurisdiction for a felony listed in section II, is disqualified until the want or warrant is released or the indictment is dismissed.

III. An individual has a disqualifying criminal offense if the individual was convicted, or found not guilty by reason of insanity, in a civilian or military jurisdiction for the following offenses, within the **past seven (7) years** from completion of sentence for the offense preceding the date of the application:

(1) Assault with intent to murder.

(2) Kidnapping or hostage taking.

(3) Rape or aggravated sexual abuse.

(4) Distribution of, possession with intent to distribute, or importation of a controlled substance.

(5) Felony arson.

(6) Felony involving a threat.

(7) Felony involving—

(i) Willful destruction of property;

(ii) Aggravated assault;

(iii) Smuggling;

(iv) Immigration violations;

(8) Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. 1961, et. seq., or a State law that is comparable, other than the violations listed in paragraph (b) of Section I.

(9) Unlawful possession, use, sale, manufacture, purchase, distribution, receipt, transfer, shipping, transporting, delivery, import, export of, or dealing in a firearm or other weapon. A firearm or other weapon includes, but is not limited to, firearms as defined in 18 U.S.C. 921(a)(3) or 26 U.S.C.5 845(a), or items contained on the U.S. Munitions Import List at 27 CFR 447.21.

(10) Conspiracy or attempt to commit any of the criminal acts listed in paragraph III.

Under want, warrant, or indictment. An applicant who is wanted, or under indictment in any civilian or military jurisdiction for a felony listed in section III, is disqualified until the want or warrant is released or the indictment is dismissed.

Level of Clearance

Up To STANDARD
Secure Access Control Areas

I. No convictions ever in your lifetime: an individual has a disqualifying criminal offense if the individual was convicted, or found not guilty by reason of insanity, in a civilian or military jurisdiction of any of the following criminal offences:

(1) Terrorism —A crime listed in 18 U.S.C. Chapter 113B—or a State law that is comparable.

(2) Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. 1961, et. seq., or a State law that is comparable.

(3) Espionage.

(4) Sedition.

(5) Treason.

(6) Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of, or dealing in an explosive or explosive device.

(7) Conspiracy or attempt to commit any of the criminal acts listed in paragraph I.

II. An individual has a disqualifying criminal offense if the individual was convicted, or found not guilty by reason of insanity, in a civilian or military jurisdiction for the following offenses, within the **past ten (10) years** from completion of sentence for the offense preceding the date of the application:

(1) Extortion.

(2) Felony involving—

(i) Theft;
(ii) Dishonesty, fraud or misrepresentation, including identity fraud and money laundering;
(iii) Unlawful sale, distribution, manufacture, import or export of a controlled substance that resulted in the conviction of an A Felony in the New York State Penal Law, or any comparable law in any State, or comparable Federal law.

(3) Conspiracy or attempt to commit any of the criminal acts listed in paragraph II.

III. An individual has a disqualifying criminal offense if the individual was convicted, or found not guilty by reason of insanity, in a civilian or military jurisdiction for the following offenses, within the **past five (5) years** from completion of sentence for the offense preceding the date of the application:

(1) Violent Felony Offenses (as defined in the New York State Penal Law §70.02) or any comparable law in any State.

(2) Conspiracy or attempt to commit any criminal act listed in paragraph III.

APPENDIX D

Secure Worker Access Consortium (SWAC)

Secure Worker Access Consortium (SWAC is accessed by an online application that enables the secure collection, processing, maintenance and real-time positive identity verification (PIV) of individuals. As of January 29, 2007, SWAC is the only Port Authority approved provider to be used to conduct background screening, except as otherwise required by federal law and or regulation. Additional information about S.W.A.C., corporate enrollment, online applications, and location of processing centers can be found at http://www.secureworker.com, or SWAC Customer Service may be contacted at (212) 608-0855.

o Consultants / Contractors

- Step 1: - A firm representative completes the Corporate Membership Application Form online at www.secureworker.com. Firms are encouraged to establish a Corporate Membership Account through which their workers will be processed.
- Step 1a: Employees & Workers of Contractors — Individual completes the Individual Membership Application Form online. (A company administrator may complete this form on someone's behalf.)
- Step 2: The applicant is photographed, provides a digital signature and presents the required identification documents at an operational SWAC Processing Center.
- Step 3: SWAC ID Card is available for pickup. The typical length of the process is one week. To verify that an ID Card is ready for pickup, call (212) 608-0855.

o Individuals

- Step 1: Individual completes the Individual Membership Application Form online. http://www.secureworker.com
- Step 2: Individual immediately takes the required government issued identity documents to a SWAC Processing Center to complete the second and final step of the SWAC application process. **NOTE**: This step is required before your background screening is initiated.

- **SWAC Processing Centers -** check the SWAC website to verify the locations, and days and times of operation of the Processing Centers.

George Washington Bridge Port Authority Administration Building, Main Lobby
220 Bruce Reynolds Boulevard
Bridge Plaza South
Fort Lee, NJ 07024
Tuesdays, 6:00 AM to 12:00PM

John F. Kennedy International Airport
Building #14
RE's Office Conference Room
Jamaica, NY
Fridays, 6:00AM to 12:00PM

Port Authority Bus Terminal
625 Eighth Avenue (at 40th Street)
South Wing, 2nd Floor
New York, NY 10018
Tuesdays & Fridays, 6:30AM to 12:30PM

LaGuardia Airport (LGA)
Port Authority Administration Building
Hanger #7S, 2nd Floor
Flushing, NY 11371
Wednesdays, 6:00AM to 12:00PM

Newark Liberty International Airport (EWR)
70 Brewster Road
Building #70 Lobby
Newark, NJ 07114
Mondays & Thursdays, 7:30AM to 3:30PM

World Trade Center
65 Trinity Place
(corner of Exchange Alley, across from SYMS clothing store)
New York, NY 10006
Monday through Friday, 6:00 AM to 12:00 PM

APPENDIX E

[insert department name] DEPARTMENT

PORT AUTHORITY OF NY & NJ

CONFIDENTIAL PRIVILEGED INFORMATION

"WARNING": The attached is the property of The Port Authority of New York and New Jersey (PANYNJ). It contains information requiring protection against unauthorized disclosure. The information contained in the attached document cannot be released to the public or other personnel who do not have a valid need to know without prior written approval of an authorized PANYNJ official. The attached document must be controlled, stored, handled, transmitted, distributed and disposed of according to PANYNJ Information Security Policy. Further reproduction and/or distribution outside of the PANYNJ are prohibited without the express written approval of the PANYNJ.

At a minimum, the attached will be disseminated only on a need to know basis and when unattended, will be stored in a locked cabinet or area offering sufficient protection against theft, compromise, inadvertent access and unauthorized disclosure.

Document Control Number: CP-[insert dept acronym]- [insert year]-[insert sequential number] – [insert copy number]

APPENDIX F

[Insert address of Recipient]

Date:

From:

The [insert department, division or project name] is providing a copy of the following items to (insert recipient's name and address).

Description	Date	Copy Number
Describe item	00/00/00	CP-[dept abbreviation]-XX-XX-XX

Upon receipt, the items listed above must be safeguarded in accordance with the procedures identified in the "The Port Authority of New York & New Jersey Information Security Handbook " dated October 15, 2008.

PLEASE SIGN AND RETURN TO:

Document Control
[insert Port Authority department, division or unit]
Attn: [SIM or SPM}
[Address]

I acknowledge receipt of the above items listed above and accept full responsibility for the safe handling, storage and transmittal elsewhere of these items.

Name (PRINT): _____

Organization: _____

Signature: _____

Date: _____

Title: _____

APPENDIX G

GUIDELINES FOR THE STORAGE OF PROTECTED INFORMATION

I. GENERAL

This section describes the **preferred methods** for the physical protection of Protected Information in the custody of PANYNJ personnel and their contractors, consultants, architects, engineers, et al. Where these requirements are not appropriate for protecting specific types or forms of such material, compensatory provisions shall be developed and approved by the Chief Information Security Officer (CISO). Nothing in this guideline shall be construed to contradict or inhibit compliance with any applicable law, statute or code. Cognizant Security Information Managers (SIM) shall work to meet appropriate security needs according to the intent of this guideline and at acceptable cost.

II. PROTECTED INFORMATION STORAGE

A. Approved Containers

The following storage containers are approved for storage of PANYNJ Protected Information:

1. A safe or safe-type steel file container that has a built-in three- position dial combination lock or electronic combination lock.

2. Any steel file cabinet that has four sides and a top and bottom (all permanently attached by welding, rivets or peened bolts so the contents cannot be removed without leaving visible evidence of entry) and is secured by a rigid metal lock bar and an approved key operated or combination padlock. The keepers of the rigid metal lock bar shall be secured to the cabinet by welding, rivets, or bolts so they cannot be removed and replaced without leaving evidence of the entry. The drawers of the container shall be held securely so their contents cannot be removed without forcing open the drawer.

B. Approved Locks and Locking Devices

The following locks and locking devices are examples of types approved for storage of PANYNJ Protected Information, but not limited to these locks:

1. Any restricted keyway 7-pin tumbler lock or equivalent pick resistant lock.

2. A combination padlock such as a Sesame four-position dial padlock. See photo at right.

For Port Authority facilities, locks and locking devices available from Port Authority stock room or approved vendor will meet this requirement.

C. Combinations to Security Containers, Cabinets, and Vaults

If required, only a minimum number of authorized persons shall have knowledge of combinations to authorized storage containers. Containers shall bear no external markings indicating the level of material authorized for storage therein.

1. A record of the names of persons having knowledge of the combination shall be maintained.

2. Security containers, vaults, cabinets, and other authorized storage containers shall be kept locked when not under the direct supervision of an authorized person entrusted with the contents.

3. The combination shall be safeguarded in accordance with the same protection requirements as the Confidential Information contained within.

4. If a record is made of a combination, the record shall be marked with the category of material authorized for storage in the container, i.e. CP or SSI.

D. Changing Combinations

Combinations shall be changed by a person authorized access to the contents of the container, or by the SIM or his or her designee. Combinations shall be changed as follows:

1. The initial use of an approved container or lock for the protection of Confidential Information.

2. The termination of employment of any person having knowledge of the combination, or when the Protected Information access granted to any such person has been withdrawn, suspended, or revoked.

3. The compromise or suspected compromise of a container or its combination, or discovery of a container left unlocked and unattended.

4. At other times when considered necessary by the SIM or CISO.

E. Supervision of Keys and Padlocks

Use of key-operated padlocks are subject to the following requirements:

1. A key and lock custodian shall be appointed to ensure proper custody and handling of keys and locks used for protection of Protected Information.

2. A key and lock control register shall be maintained to identify keys for each lock and their current location and custody.

3. Keys shall be inventoried with each change of custody.

4. Keys and spare locks shall be protected equivalent to the level of classified material involved.

5. Locks shall be replaced after loss or compromise of their operable keys.

6. Making master keys is prohibited.

F. Document Retention Areas

Due to the volume of the Protected Information in possession, or for operational necessity, it may be necessary to construct Document Retention Areas for storage because approved containers or safes are unsuitable or impractical. Access to Document Retention Areas must be controlled to preclude unauthorized access. During hours of operation this may be accomplished through the use of a cleared person or by an approved access

control device or system. Access shall be limited to authorized persons who have an NDA on file, received appropriate training on the protection of information and have a bonafide need-to-know for the Protected Information material/information within the area. All other persons (i.e. visitors, maintenance, janitorial, etc.) requiring access shall be escorted at all times by an authorized person where inadvertent or unauthorized exposure to Protected Information cannot otherwise be effectively prevented. During non-working hours and during working hours when the area is unattended, admittance to the area shall be controlled by locked entrances and exits secured by either an approved built-in combination lock, an automated access control system or an approved key-operated lock. Doors secured from the inside with an emergency panic bar will not require additional locking devices.

G. Construction Requirements for Document Retention Areas

This paragraph specifies the minimum safeguards and standards required for the construction of Document Retention Areas that are approved for use for safeguarding Protected Information. These criteria and standards apply to all new construction and reconstruction, alterations, modifications, and repairs of existing areas. They will also be used for evaluating the adequacy of existing areas.

1. **Hardware:** Only heavy-gauge hardware shall be used in construction. Hardware accessible from outside the area shall be peened, pinned, brazed, or spot welded to preclude removal.

2. **Walls:** Construction may be of material offering resistance to, and evidence of, unauthorized entry into the area. If insert-type panels are used, a method shall be devised to prevent the removal of such panels without leaving visual evidence of tampering.

3. **Windows:** During nonworking hours, the windows shall be closed and securely fastened to preclude surreptitious entry.

4. **Doors:** Doors shall be constructed of material offering resistance to and detection of unauthorized entry. When doors are used in pairs, an astragal (overlapping molding) shall be installed where the doors meet.

5. **Ceilings:** Where surrounding walls do not extend to the true ceiling, the ceiling shall either be hard capped with the same construction materials as the surrounding walls or removable tiles shall be clipped in place such that they cannot be removed without destroying tiles and providing evidence of intrusion.

APPENDIX H

GUIDELINES FOR THE DISPOSAL AND DESTRUCTION OF PROTECTED INFORMATION.

I. GENERAL

This section describes the preferred methods for the disposal and destruction of Protected Information in the custody of PANYNJ personnel and their contractors, consultants, architects, engineers, et al. Where these requirements are not appropriate for disposal or destruction of specific types or forms of such material, compensatory provisions shall be developed and approved by the Chief Information Security Officer (CISO). Cognizant Security Information Managers (SIM) shall work to meet appropriate security needs according to the intent of this guideline and at acceptable cost.

Protected Information no longer needed shall be processed for appropriate archiving or disposal. Protected Information approved for destruction shall be destroyed in accordance with this section. The method of destruction must preclude recognition or reconstruction of the Protected Information or material.

All persons in possession of Protected materials shall establish procedures for review of their Protected holdings on a recurring basis to reduce these inventories to the minimum necessary for effective and efficient operations. Multiple copies, obsolete material, and Protected waste shall be destroyed as soon as practical after it has served its purpose. Any appropriate downgrading actions shall be taken on a timely basis to reduce the volume and to lower the level of Protected material being retained.

Original records must be retained in accordance with the Agency's Records Management Policy and Retention Schedules.

II. DISPOSAL AND DESTRUCTION

A. Destruction Requirements

All persons in possession of Protected materials shall destroy this material in their possession as soon as possible after it has served the purpose for which it was released, developed or prepared, or as soon as possible after its designated retention period has expired.

B. Methods of Destruction

1. Generally, Protected material shall be destroyed by commercial grade cross cut shredders located conveniently throughout the workplace for use by authorized individuals.

2. Additionally, Confidential material may be destroyed by burning, pulping, melting, mutilation, chemical decomposition, or pulverizing (for example, hammer mills, choppers, and hybridized disintegration equipment) where shredding may not be appropriate. Whatever method is employed must preclude recognition or reconstruction of the Confidential Information or material.

3. Confidential material in microform, that is: microfilm, microfiche, or similar high data density material, may be destroyed by burning or chemical decomposition, or other methods as approved by the CISO.

4. Commercial destruction facilities may be used only with the approval of, and under conditions prescribed by, the SIM. When commercial destruction facilities are utilized, they shall conform to all appropriate sub-contracting requirements to include appointment of a SIM, adherence to the requirements of the PANYNJ Information Security Handbook, receiving required security training and properly executing a Non-Disclosure and Confidentiality Agreement (NDA).

5. Electronically Stored Protected Information must be deleted from all computer hard drives, tapes, CD's, DVD's, memory, and/or magnetic, analog, or digital media used to store or transport digital files. The device used to store or transport any Protected file will require a bit-by-bit overwrite of the storage area used by the file. This will protect against having the deleted file recovered using data recovery tools. Commercial tools are available to automate this process.

C. Witness to Destruction

Protected material shall only be destroyed by authorized personnel, whether in-house or contracted, who meet all of the PANYNJ criteria for awarding access authorization, have met all training requirements, have a properly executed NDA on file and have a full understanding of their responsibilities to ensure proper control of the materials while in their possession and complete destruction thereof.

D. Destruction Records

Protected Information is accountable and therefore any disposal in approved waste containers or destruction via convenience shredders must be reported to the issuing SIM, or his/her document control representative, indicating which documents were disposed/destroyed and the date of such action.

Protected waste shall be destroyed as soon as practical. This applies to all waste material containing Protected Information. Pending destruction, Protected waste shall be appropriately safeguarded. (See also Appendix G - Guidelines for the Storage of Protected Information.)

III. PROTECTED WASTE

A. Approved Receptacles

1. Receptacles utilized to accumulate Protected waste shall be constructed of substantial materials that would provide evidence of tampering. Hinges and lids shall not be removable while the container is secured without leaving evidence thereof.

2. All such receptacles shall be clearly identified as containing Protected material.

3. Slots shall be provided in such receptacles that allow for easy deposit of materials for destruction but preclude removal of deposited waste by insertion of a person’s hand or tool.

4. Locks, and the control thereof, on all Protected waste receptacles shall meet or exceed the requirements of the PANYNJ Guideline for Storage of Confidential Information.

B. Oversize Waste Materials

PANYNJ projects often involve large drawings and other materials associated with construction projects, which cannot be conveniently disposed of via office shredders or placed in typical slots on secure trash receptacles. In no cases shall such material be permitted to be placed or accumulate adjacent to secure receptacles while awaiting destruction. Oversize materials awaiting destruction may be stored as follows:

1. Within an approved Document Retention Area.

2. Within a specially constructed secure waste receptacle where disposal slots have been specifically designed for accepting rolled drawings or other oversize materials and preclude the removal there from.

3. Within a standard secure waste receptacle where the receptacle has been opened by an authorized individual to allow placement of the oversized item(s) into the container and it has been secured thereafter.

APPENDIX I

Audit Procedures

COMPANY / ORGANIZATION

- Is the Company Non-Disclosure and Confidentiality Agreement properly executed and maintained in current status?
- Has a senior management official been designated as Security Information Manager (SIM), as required by the Handbook for Protecting Security Information? Has a deputy SIM been identified?

ACCESS AUTHORIZATIONS

- Has a Non-Disclosure Agreement been executed by each employee who has been afforded access?
- Is a current record maintained of all employees authorized access to Confidential Information at the firm?
- Does the contractor provide a roster of all cleared employees to the PA as required? Is it current?

SECURITY EDUCATION

- Does the contractor provide that all employees who have access to Protected Information with security training and briefings commensurate with their involvement with the information?
- Are contractors who employ persons at other locations ensuring the required security training?
- Are the Non-Disclosure Agreements executed by employees prior to accessing the sensitive information?
- Do initial security briefings contain the minimum required information?
- Does the contractor's security education program include refresher security briefings?
- Are employees debriefed at the time of a termination, reassignment or project's completion regarding the requirements for continued safeguarding of Protected

Information?

- Has the contractor established internal procedures that ensure authorized awareness of their responsibilities for reporting pertinent information to the SIM?
- Has the contractor established a graduated scale of administrative disciplinary action to be applied against employees who violate the Handbook?
- Are employees aware of Emergency Procedures?
- Does management support the program for safeguarding Port Authority Confidential and Privileged Security Information?

STANDARD PRACTICE PROCEDURES

- Is the Confidential Information Practice and Procedures ("CIPP") document current and does it adequately implement the requirements of the Handbook?
- A CIPP only needs to be prepared when the Departmental Information Security Officer ("DISO") believes it necessary for the proper safeguarding of Confidential Information.

SUBCONTRACTING

- Have all Subcontractors properly executed the Non-Disclosure and Confidentiality Agreement?
- Has a Non-Disclosure Agreement been executed by each of the Subcontractor's employees who has been afforded access?
- Is a current roster maintained of all Subcontractor employees authorized access to Confidential Information at the firm?
- Does the Subcontractor provide this roster to the Prime Contractor's SIM as required? Is it current? Does it include the date that the agreement was signed? Is it included in the Prime Contractor's Team Roster?
- Does the contractor complete all actions required in the Handbook prior to release or disclosure of Port Authority Protected Information to subcontractors? Has the Subcontractor been provided a Handbook?
- Has a senior management official of the Subcontractor been designated as the Security Information Manager (SIM), if required by a CIPP?

- Has a deputy SIM been identified?
- Is the safeguarding capability of all subcontractors determined as required?
- Is the requirement to abide by security procedures identified in the Handbook incorporated into each subcontract?
- Does the Subcontractor have an adequate understanding of the Handbook's requirements and the types of information that require safeguarding?

VISIT CONTROL

- Are procedures established to ensure positive identification of visitors prior to disclosure of Protected Information?

CLASSIFICATION

- Does the contractor have adequate procedures for evaluating Protected material being created, extracted, or summarized?
- Is contractor-developed Protected Information appropriately marked, and protected?

PUBLIC RELEASE

- Does the contractor obtain the approval of the Port Authority prior to public disclosure of *ANY* information pertaining to a security program contract?

STORAGE

- Has the contractor established a system of security checks at the close of each working day to ensure that sensitive material is secured?
- How would the Protected material be safeguarding during an emergency?
- Is a record of the names of persons having knowledge of the combinations to security containers maintained?
- When combinations to containers are placed in written form, are they stored appropriately?
- Do authorized persons, when required, change combinations to security

containers?

MARKINGS

- Is all Protected material, regardless of its physical form, marked properly?
- Is all Protected material marked to show the name and address of the facility responsible for its preparation and the date of preparation?
- Are overall markings marked conspicuously as required?
- Are protective markings applied to Protected compilations if required?

TRANSMISSION

- Is Protected Information properly prepared for transmission outside the facility?
- Are Transmittal Receipts included with Protected Information if required?
- Is a suspense system established to track transmitted documents until the signed receipt is returned?
- Are authorized methods used to transmit Protected material outside the facility?
- Is the NDA of the receiving facility determined prior to transmission of Protected Information?

PROTECTED INFORMATION CONTROLS

- Do contractor employees understand their safeguarding responsibilities?
- Is the contractor's accountability system capable of facilitating the retrieval and disposition of Protected material as required?
- Are external receipts and dispatch records maintained as required?
- Is all Protected material received at the contractor facility and delivered directly to designated personnel?
- Do contractor employees promptly report the loss, compromise, or suspected

compromise of Protected Information to the SIM?

DISPOSITION

- Is a program established to review Protected retention on a recurring basis for the purpose of reduction?
- Is Protected material destroyed as soon as possible after it has served its purpose?
- Does the contractor employ an effective method of destruction?
- Is Protected material destroyed by the appropriate employees?
- Is Protected waste properly safeguarded until its timely destruction?

REPRODUCTION

- Does the facility's reproduction control system keep reproduction of Protected material to a minimum?
- Is the reproduction of Protected Information accomplished only by properly authorized, and knowledgeable employees?
- Is reproduction authorization obtained as required?
- Are reproductions of Protected material reviewed to ensure that the markings are proper and legible?

AUTOMATED INFORMATION SYSTEMS (AIS)

- Are appropriate physical controls being exercised over approved AIS?
- Are AIS media containing Protected Information handled in a manner consistent with the handling of Confidential documents?
- Are all AIS storage media, internal memory, and equipment, that contain Protected Information, properly sanitized prior to removal from protection?

Suggested Questions When Interviewing Employees NOT Authorized Access to Confidential Information:

- What is Protected Information?
- Have you ever seen Protected Information?
- If you found Protected Information unprotected, what would you do?

Suggested Questions When Interviewing Employees Authorized Access to Protected Information:

- What is your job title/responsibility?
- Which contract or program requires you to access this information?
- How do you access the information?
- How long have you been authorized access?
- When was your last access to Protected Information?
- Have you ever had access to Protected Information outside of this facility?
- Did anyone else from the facility accompany you?
- Did you take any Confidential notes or Protected Information back to the facility?
- What procedures were followed to protect this information?
- Where is this information now?
- Have you ever provided access to Protected Information to visitors?
- How did you determine their need-to-know?
- Have you ever been approached by anyone requesting Protected Information?
- Do you ever work overtime and access Protected Information?
- When was the last time that you had a security briefing?
- What can you recall from this briefing?
- Have you ever been cited for a security violation?
- What would YOU do if YOU committed a security violation or discovered one?
- Do you have the combination to any storage containers?
- Who other than yourself has access to these containers?

- Is a record maintained of the safe combination? If so, where?
- Do you reproduce or generate Protected Information?
- Where do you typically work when you generate Protected Information?
- What procedures do you follow to protect Protected Information while working on it?
- Do you ever use a computer to generate Protected Information? How do you mark this Information?
- Please produce the guidance that you used. Is it accurate?
- What procedures do you employ when hand carrying Protected material?
- Have you reproduced Protected Information? Describe the procedures.
- Have you destroyed Protected Information? What procedures were used?
- Do you have any questions regarding security?

Parking Access and Revenue Control System—Design, Installation & Maintenance

Attachment P
Submittal Requirements

Attachment P—Submittal Requirements

For assistance to Proposers, the below is a list of submittals referenced in Attachment D—Scope of Work. This list is provided as a minimum standard that Proposers shall Propose and the Port Authority is not responsible if this list is not complete.

Title	**Description**	Submitted? Y/N	If No, why not
Installation & Implementation Schedule	The installation of the New PARCS shall be delivered in four installments related to the four airports. An efficient cost-effective development and installation schedule should be submitted along with backup information as to why it differs from the Authority's proposed schedule.		
Migration Plan	A comprehensive detailed phasing plan and methodology to accomplish the transition from the Existing PARCS to the New PARCS.		
Preventative Maintenance Tasks and Schedule	Details of the necessary Preventive Maintenance Tasks for the New PARCS.		
Maintenance Staff Resumes	Resumes for the proposed maintenance staff.		
Contractor Job Descriptions	Detailed job descriptions for all positions involved in maintaining the Existing PARCS as well as descriptions for those designing, installing and maintaining the New PARCS.		
Numbers and Hours of Technicians	Anticipated on-site hours and typical numbers of technicians on-site at any one time during the installation of the New PARCS.		
Warranty Coverage	Details concerning warranty coverage of New PARCS equipment.		
New PARCS System Testing Plan	a plan for the Factory Acceptance Test, Site Acceptance Test and Operational Acceptance Test		
Training Plan	A Training Plan shall be provided by the Contractor in order to provide initial Train the Trainer program for all users of the Parking Access and Revenue Control System.		

For assistance to Proposers, the below is a list of submittals referenced in Attachment E—Functional Specifications. This list is provided as a minimum standard that Proposers shall Propose and the Port Authority is not responsible if this list is not complete.

Title	Description	Submitted? Y/N	If No, why not
Pricing Sheets	Contractors shall provide separate pricing for all proposal items as outlined in Attachment C2.		
Software List	Contractor shall identify each software package it intends to use including:		
Software List	Any and all third party software and their associated licenses and manufacturer's support services		
Software List	Each industry standard software packages Contractor intends to use shall be identified. The Contractor's Proposal shall state the purpose of the software package, where it shall be used, and how it shall be used.		
Software List	Contractor shall identify the version of PARCS and PSCS software that shall be used		
Data Reporting Formats	Contractor shall identify what formats are acceptable for the data reporting system and the means for incorporating the data		
Test Equipment	Contractor shall notify the Authority of all test equipment necessary to support the PARCS.		
Host Standby Server Solution	Contractor shall provide requirements to the Port Authority (according to Port Authority IT standards) for a host standby server solution that provides high availability and redundant data storage. Contractor shall provide the appropriate management software package.		
Fees	Contractor shall submit the pricing structure for any		

	related credit card, chip and PIN card, pay-by-phone or gateway fees that shall be incurred.		
Entry Stations	Contractor shall submit product data of proposed Entry Stations, including sample Entry Station active color matrix message screen that is easily readable in all ambient lighting conditions.		
Cashier Stations	Contractor shall submit product data of proposed Cashier Station CCTV and Audio/Visual Functionality.		
Express Exit Stations	Contractor shall submit product data of proposed Express Exit Stations.		
Barrier Gates	Contractor shall submit product data of all proposed barrier gates.		
Lane Signs	Contractor shall submit product data of the proposed Lane Open/Closed Signs.		
UPS Devices & Software	Contractor shall submit specification sheets of all proposed UPS devices and UPS monitoring software.		
Dynamic Signage	Contractor shall submit product data and photographs of all proposed PSCS Dynamic Signage.		
LPR Solution Including Server Locations	Contractor shall propose an LPR solution which indicates whether to locate LPR servers centrally or at the lanes.		
LPR Camera Product Data	Contractor shall submit product data of the proposed LPR cameras.		
Vehicle Detection	Space-By-Space Vehicle Detection, Contractor shall provide quantities of equipment, locations and costs for the total hardware, licensing and software needed each category: Space by Space; Row		
Intercom Information	Contractor shall submit product data of the intercom base station and push button intercom terminals.		
Validation Stations	Contractor shall submit a cut sheet of the proposed Validation Stations		
LPI Handhelds	Contractor shall submit product data of all proposed LPI Handhelds		
APS Information	Contractor to provide the Authority with electrical and		

	communications requirements for Automated Pay Stations (APS) devices that are integrated into the PARCS.		
POF Pricing	Contractor shall provide pricing in their proposal for credit card only POF and cash/credit card POF		
EZ-Pass® Plus™ Integration Information	Contractor's proposal must include the equipment and functionality to use a valid *E-ZPass®Plus™* transponder to enter or exit through all lanes		
RFID Information	bidder shall provide details for RFID Transponder system installation and functionality		
Scalability Plan	Vendors are required to set out exactly how their proposals will accommodate a) significant increases in volumes of transactions at all Port Authority airport parking lots and b) numbers of parking lots on the system both real and virtual		
Development Cost	cost structure and delivery timeline for any Port Authority development services		

Parking Access and Revenue Control System—Design, Installation & Maintenance

Attachment Q
Example Change Control Management Submission Form

Example Change Control Management Submission Form

Start Date:	
Start Time:	
End Date:	
End Time:	
Title:	
Short Description:	
Long Description*:	
Reason(s) for Change:	
Customer Impact: (Indicate Dept/User)	
Potential Risk: (Indicate impact if change failed)	
Customer Notified By:	
Contact Person(s):	
Comment*:	
Submitted By:	
Approved By:	

* Designates optional field. All other fields are required.

NOTES:

All fields, except those in blue (Long Description, Comment) MUST be filled in, completely.

The following fields will be displayed for the entire Agency general public:

Start Date, Start Time, End Date, End Time, Title, Short Description, Reason(s) for Change, Impact, Contact Person(s).

Descriptions and information provided should be appropriate for the general audience.

To submit your change event:

1. Fill out this Change Control Management Submission Form in its entirety.
2. Save the document as follows: CCMSF_[email-alias]_[today's date mmddyy]. Example: CCMSF_jsmith_080206.
3. Submit to TBD for approval, and once approved then
4. Attach the saved document to an e-mail with a Subject line of "Change Control Submission" and send it to TBD.

Parking Access and Revenue Control System—Design, Installation & Maintenance

Attachment R
Existing System Preventative Maintenance Schedule

PM Procedures For Cashier Terminal (CT)
To Be Performed Every Two Weeks

Lane Checks and Service	Period
Perform visual inspection for mechanical, electrical, loose connection or corrosion damage. And verify voltages are within acceptable parameters.	Each PM
Blow out dust or dirt with compressed air	Each PM
Check to ensure all digits of the Patron Fee Display are functioning. Clean PFD	Each PM
Clean and service ticket reader and replace printer ribbon if necessary.	Each PM
Visually inspect magnetic heads , clean rollers,belts of ticket transport	Each PM
Check for proper loop detector operation.	Each PM
Clean and service receipt printer if necessary.	Each PM
Clean and Calibrate Optical trigger if necessary (using rain ex etc.)	Each PM
Clean keyboard and monitor; check functionality of keys on keyboard.	Each PM
Clean and service gate mechanism and gate arm. Check to ensure fans and internal components are free of dust and debris.	Each PM
Check/calibrate sonic sensor (sensor must be connected)	Each PM
Check serviceability of gate and gate arm. Check for loose or damaged wires and cables, missing screws, and proper voltages.	Each PM
Check/replace floodlights as necessary.	Each PM
Check serviceability of cash drawers. Ensure cash drawer opens and closes easily.	Each PM
Check CT's Emergency Function. Ensure both cash drawers and gate opens.	Each PM
Clean and service camera housing and camera lens. Check to ensure camera is mounted securely. Check for loose or damaged cables. Check alignment	Each PM
Check/Align LPR camera with test jig	Each PM
Check Intercom.	Each PM
Check/verify EZ — pass operation where applicable. Overhead and patch	Each PM
Stop APS - init 6	Each PM

PM Procedure For Employee Lots
To Be Performed Every Two Weeks

Lane Checks and Service	
Perform visual inspection for mechanical, electrical, loose connection or corrosion damage.	Each PM
Blow out dust or dirt with compressed air	Each PM
Check to ensure all digits of the Patron Fee Display are functioning. Clean PFD	Each PM
Visually inspect the internal components of the lane equipment for loose connections or damage and verify voltages are within acceptable parameters.	Each PM
Check for proper loop detector operation.	Each PM
Check UPS	Each PM
Clean and service gate mechanism and gate arm. Check to ensure fans and internal components are	Each PM
Check/calibrate sonic sensor (sensor must be	Each PM
Check serviceability of gate and gate arm. Check for loose or damaged wires and cables, missing screws,	Each PM
Stop APS — init 6	Each PM

PM Procedures For Ticket Issuing Machine (TIM) To Be Performed Every Two Weeks

Lane Checks and Service	Period
Perform visual inspection for mechanical, electrical, loose connection or corrosion damage.	Each PM
Blow out dust or dirt with compressed air	Each PM
Clean and service ticket reader and replace ribbon if necessary.	Each PM
Visually inspect magnetic heads, clean rollers, and belts of ticket transport. replace if necessary.	Each PM
Visually inspect the internal components of the lane equipment for loose connections or damage and verify voltages are within acceptable parameters.	Each PM
Check for proper loop detector operation.	Each PM
Clean and service receipt printer if necessary.	Each PM
Clean and Calibrate Optical trigger if necessary (using rain ex etc.)	Each PM
Check to ensure UPS And Heater works	Each PM
Clean and service gate mechanism and gate arm. Check to ensure fans and internal components are free of dust and debris.	Each PM
Check/calibrate sonic sensor (sensor must be connected)	Each PM
Check serviceability of gate and gate arm. Check for loose or damaged wires and cables, missing screws, and proper	Each PM
Check/replace floodlights as necessary.	Each PM
Clean and service camera housing and camera lens. Check to ensure camera is mounted securely. Check for loose or damaged cables. Check alignment	Each PM
Check/Align LPR camera with test jig	Each PM
Check Intercom.	Each PM

PM Procedures for FOIC To Be Performed Every Two Weeks

Lane Checks and Service		
Perform visual inspection for mechanical, electrical, loose connection or corrosion damage.	Each PM	
Blow out dust or dirt with compressed air	Each PM	
Check to ensure UPS works	Each PM	
FOIC Cabinet		
Check cables/connection	Each PM	
Check AC/heat operation	Each PM	
Check Media Converter connections where applicable		
Check Cisco Connections		

Parking Access and Revenue Control System—Design, Installation & Maintenance

Attachment S
Spare Parts Inventory

Approved by PA:_____

LGA Spare Parts Inventory - October 2014

Part Number	Description	Rec level	Maintenance Spares SRO	On Hand	Total	COMMENTS/SRO
11-3914	Pushbutton Lightbulbs	0		14	**14**	**Consumable**
01-40008	Sonet Node 10/100 Ethernet card	0	0	0	**0**	**Don't use**
10-25312	Cable - harness,button light-tid and act	4	0	4	**4**	
10-25315	Display/IR Cable	5	0	6	**6**	
10-25346	Cable - Ticket Dispensor / POF	2		3	**3**	
10-25348	cable td400 display cable for TID	2		1	**1**	**ordering 1**
10-26252	Cash Drawer Cables	4	0	4	**4**	
11-0003	T Handle lock w/key	5	0	6	**6**	
11-11307	24vdc fan cover	5	0	10	**10**	
11-11785	24VDC Fan	5	0	8	**8**	
11-12262	Ultra Sonic Safety Sensor	10		6	**6**	**Testing out alternate**
11-1743	5 amp fuses	10	0	20	**20**	
11-25027	Lock Assembly spitter doors	7		2	**2**	
11-25159	Patron Credit Card Reader (ACT)	10		10	**10**	
11-25178	Check Combo Reader	5		7	**7**	
11-25180	ACT Printer (Ithaca)	5		8	**8**	
11-25202	ELO Touchscreen	5		8	**8**	
11-25224	Cash Drawer	4		4	**4**	**ABM to replace broken insert 2**
11-25258	Sun keyboard type 6	10		8	**8**	**Consumable -ABM**
11-25489	DB9 terminal adapter, 1 req'd per P357 trigger input	2		2	**2**	
11-25510	Fuse Posi Drive Gate	10		0	**0**	**15 on order**
11-25511	Gate fuse holder	2		2	**2**	
11-25582	Floodlight 45W halogen	0		0	**0**	**Consumable**
11-25583	Floodlight fixture, dual	1		0	**0**	**ordering 1**
11-25681	check combo rdr cable	5		9	**9**	
11-25803	Sapphire, PANYNJ, configured w/sftwr & drivers	13		6	**6**	**Researching**

11-25839	Novus 2 UPS w/extd alarm card (may run from adj. lane UPS)	1		0	**0**	**Used for lot 5 Hurricane Sandy**
11-25844	Pin pad (ACT)	5		10	**10**	
11-25879	Cisco Switch	1		3	**3**	
11-25926	Filters	0		0	**0**	
11-25982	Null modem adapter	1		1	**1**	
11-25989	Check/combo rrdr power supply	5		4	**4**	
11-26011	Cat5 patchcord, 2 meter	4		0	**0**	**make 4**
11-26099	16 Port Dlink Switches	2	2		**2**	**Sro**
11-26185	Perle (EZ Pass)	4		4	**4**	
11-26377	POF MONITOR	3	1	2	**3**	**Sro**
12-10417	Universal Power Supply	4		4	**4**	
12-10424	Comm Gateway Controller	10		12	**12**	
12-10438	In-booth Mag Stripe Ticket Reader	10		10	**10**	
12-10439	RB Intercom w/outdoor quad box	2			**0**	**looking for**
?	DB9-RJ12 Connector	5		12	**12**	
12-10451	DB9F to RJ45 adapter, 1 req'd per VMS	5		3	**3**	**used 2 for lot 5 hurricane sandy**
12-10453	HID READ HEAD	2		2	**2**	
12-25268	LPR/CCTV post w/L-bracket, U bolt, & (3) 4" caps	0		0	**0**	
20-11903	Main Shaft Crank	10		10	**10**	
20-11907	Motor Crank (Posidrive gate)	4		4	**4**	
20-11922	main spring pivot bar	4		4	**4**	
20-11924	Gate Spring	10	5	5	**10**	**SRO**
20-12186	Red reflective tape	2		2	**2**	
20-3469	Gate Warning labels	10		0	**0**	**Researching**
21-11921	Bearing Spring Crank	5		5	**5**	
21-11944	Posi Gate Switch (door)	5		3	**3**	
30-22073	Patron CC rdr cable	6		0	**0**	**order**
30-25976	Retracted Ticket Bins	2		1	**1**	**JFK needed 1**
30-26419	exit transport deflector	0		0	**0**	
30-26478	ACT cabinet tabs	0		0	**0**	
32-22361	TD420 Controller	8		5	**5**	
32-22362	TD400 Field I/O Assembly	10		13	**13**	

32-22364	Exit Transport (verifier)	12		10	**10**	
32-22365	TD 420 Transport Assembly (Dispenser)	13		7	**7**	
32-22408	POF Transport	3		1	**1**	
32-25207	Issuing Device	0		2	**2**	
32-25208	Center stripe ASCOM module	0		4	**4**	
41-17102	Power Supplies (ACT)	5		6	**6**	
41-25652	Receipt Buttons	2		1	**1**	**ordering**
42-16866	POF reciept printer	2		1	**1**	**ordering**
50-14048	Warning Label	5			**0**	**check syteline**
50-25072	Connecting Rod (Narrow)	3		3	**3**	
50-25101	Gate Arm end cap	10		10	**10**	
50-25102	Gate Anti-Slip Insert	10		42	**42**	
50-25112	Gate Arms 10ft	5		10	**10**	
51-25110	Gate Motors (Bodine DC motor)	2		3	**3**	
52-14053	LCD Display Interface	10		11	**11**	
52-14056	Posi Drive Controller	15		22	**22**	
52-14087	BRO-1 Buffer relay pkg (R/G light control)	1		1	**1**	
53-14001	Gate Drive Assembly (complete -motor,power supply and mech)	3		3	**3**	
53-14073Y	Complete Gate	1		1	**1**	
60-26063	Prox intercom mtg plate	0		0	**0**	
62-15672	IP Dongles	5		4	**4**	**ordering**
63-15732	HID MaxiProx reader w/Non-metallic Jbox, 8x8x4	0		0	**0**	
80-20491	Push for ticket Buttons	2		1	**1**	**ordering**
80-20492	Cancel Buttons	2		1	**1**	**ordering**
80-22386	cable -Display cable ACT	5		5	**5**	
80-22387	pin pad cable	5		5	**5**	
80-22388	cable - TD400 mag cable	2		5	**5**	
80-22391	patron receipt printer cable	2		1	**1**	**ordering**
80-25356	40 pin ribbon cable I/O to td-400 controller	5		8	**8**	
82-20059	LCD - Display	12		12	**12**	
82-22078	ACT fan filter w/cover	5		10	**10**	
82-22383	Receipt Printer (Patron)	5		7	**7**	

87-19688	52 pin ribbon cable -(ACT) td400 to transport)	5		30	**30**	
CCTV-0004	Spectralite outdoor PTZ color camera	5		4	**4**	**looking for**
CCTV-0006	Spectra outdoor wall pendant w/PS	2		2	**2**	
CCTV-0009	Video server, Axis 2400+	3		6	**6**	
LPR-0001	P357 Image processor, PANYNJ (PIPs Server)	8	1	7	**8**	**Hurricane Sandy**
LPR-0004	LPR camera connector	0		0	**0**	
LPR-0005	LPR Optical Trigger	25	2	23	**25**	**SRO**
LPR-0036	Sgl Lane Optical Trigger/Reflector assm w/stands	4		4	**4**	
LPR-0044	LPR P356 camera w/swivel brackets & mtg hardware	0		0	**0**	
LPR-0045	P356 LPR 810nm camera w/5-50 varifocal lens, long hood	9		9	**9**	
LPR-0062	Dual Lane Optical Trigger PVC enclosure upgrade	0		0	**0**	
NPN	EzPass patch reader mushroom cap (green)	5		5	**5**	
NPN	adj thermostat	1		0	**0**	
NPN	gate motor keys	10		59	**59**	
NPN	Photo Cell	1		0	**0**	
NPN	CCTV Camera Domes	2		2	**2**	
VMS-0019	VMS 1226-2 wall mtd 1.5" char. 2 line Red LED sign	2		2	**2**	
VMS-0020	VMS mtg bracket, PA version w/clamps & mtg hardware	0		0	**0**	

3M PARTS INVENTORY - JFK International Airport (Sept. 2015)

Part Number	Description	Required Stock Level	Maintenance Spares Breakdown				Notes
			Depot Repair	On Hand	Total	Re-Order	
Cashier Terminal, ACT, POF Gate Cabinet							
11-25202	ELO Touchscreen	2	4	2	6	2	
11-25180	CT Printer (Ithaca)	3	2	1	3	2	
11-25178	Check Combo Reader	3	1	6	7	2	
11-25224	Cash Drawer	3		3	3	2	
32-22361	TD400 Controller	5	3	16	19	5	
52-14056	Posi Drive Controller	5	5	13	18	5	
12-10424	Comm Gateway Controller	5		8	8	3	
31-12511	Printer Ribbon Cartridge, TD400						*Consumable supplied by ABM*
32-22362	TD400 Field I/O Assembly	5		12	12	5	
32-22365	TD 420 Entrance Transport Assembly	6	2	10	12	4	
	Retracted Ticket Bins	2		3	3	2	
32-22364	TD 420 Exit Transport Assembly	6	6	11	17	4	
30-25749	Ticket Deflector Plate				0		*Located on each part 32-22364*
32-22408	TD 420 POF Transport Assembly	1		1	1	3	*Can be interchanged with part 32-22364*
11-26377	POF Monitor	2	1	1	2	1	*1 out for repairs*
11-25159	POF Credit Card Reader	1		1	1	2	*interchangeable with part 11-25159*
52-14053	LCD Display Interface	5		10	10	2	
82-20059	LCD - Display	2		6	6	2	
82-22383	ACT Receipt Printer (Patron)	4	3	4	7	2	
11-12262	Ultra Sonic Safety Sensor	6		2	2	2	
51-25110	Gate Motors (Bodine DC Motor)	4	4	16	20	3	
50-25403	Main Spring Posi 50	10		2	2	5	*additional To be ordered*
80-20491	Push for Ticket Buttons	3		5	5	2	
41-25652	Push for Receipt Buttons	3		5	5	2	
11-3914	Pushbutton Lightbulbs	5		15	15	5	
53-14001	Gate Drive Assembly	2		2	2	1	
11-25510	20 Amp Fuse Posi Drive Gate	5		6	6	3	
50-25072	Connecting Rod (Narrow)	4		7	7	4	
20-11903	Main Crank Shaft Pt 1 (Posidrive Gate)	4		4	4	2	
20-11920	Spring Crank (Posidrive Gate)	4		10	10	2	
20-11907	Motor Crank (Posidrive Gate)	4		2	2	3	
21-11921	Bearing Spring Crank	4		4	4	2	
21-11944	Posi Gate Switch (Posidrive Gate)[Door]	2		4	4	1	
12-10417	Universal Power Supply	2		4	4	1	
50-25112	Gate Arms 10ft	2		2	2	5	*30 additional in transit from Texas*
50-25101	Gate Arm end cap	4		6	6	3	*On gate arm*
62-15672	IP Dongles	2		4	4	5	
11-0003	T Handle lock w/key	2		8	8	3	
11-1743	5 Amp Fuse	5			0	3	
11-25159	Patron Credit Card Reader (ACT)	2		2	2	2	
41-17102	Power Supplies (ACT)	3		5	5	3	
11-25844	Pin pad (ACT)	2		2	2	2	

3M PARTS INVENTORY - JFK International Airport (Sept. 2015)

Part Number	Description	Required Stock Level	Maintenance Spares Breakdown				Notes
			Depot Repair	On Hand	Total	Re-Order	
Cashier Terminal, ACT, POF Gate Cabinet							
11-26099	16 Port Dlink Switch	2		9	9	3	
11-25027	Lock Assembly spitter doors	2		4	4	3	
11-25258	Sun keyboard type 6-7	0		0	0	2	*Keyboards supplied by ABM*
11-25489	DB9 terminal adapter, 1 req'd per P357 trigger input	1		1	1	1	
11-25583	Floodlight fixture, dual				0	1	
11-25803	Sapphire, PANYNJ, configured w/sftwr & drivers	5		11	11	5	
11-25839	Novus 2 UPS w/extd alarm card	1		1	1		
11-11785	24VDC Fan				0	2	
12-10438	In-booth Mag Stripe Ticket Reader	2		2	2	2	
11-26185	Perle (Kapsch IV)	2		3	3	2	
800260-007	IAG-2T 007 Antenna (Kapsch IV)	1		1	1		
800260-008	IAG-2T 008 Antenna (Kapsch IV)				0		
12-25268	LPR/CCTV post w/L-bracket, U bolt, & (3) 4" caps						*This is not an item frequently used. Only in a severe instant like a vehicle running it over*
52-14087	BRO-1 Buffer relay pkg (R/G light control)	2		2	2	1	
11-12238	HID MaxiProx Reader	2		4	4	2	
11-25879	Cisco Switch	1		3	3	1	
VMS-0019	VMS 1226-2 wall mtd 1.5" char. 2 line Red LED sign	2		1	1	2	
12-10451	DB9F to RJ45 adapter, 1 req'd per VMS	2		1	1	1	
12-10451	DB9-RJ12 Connector	2		2	2	1	
	UPS Battery	0		1	1		*1 set =4 batteries. 3 represents 3 sets of 4 batteries*
63-15713	II3 Intercom Assy	1		3	3	1	
12-10439	RB Intercom w/outdoor quad box	1		1	1	1	
License Plate Recognition							
NPN	CCTV Camera Domes	2		2	2	1	
CCTV-0004	Spectralite outdoor PTZ color camera	2		2	2	1	
CCTV-0006	Spectra outdoor wall pendant w/PS	3		6	6	3	
CCTV-0009	Video server, Axis 2400+	2		4	4	2	
LPR-0001	P357 Image processor, PANYNJ ALPR Image Processor	4	3	6	9	2	
LPR-0004	LPR camera connector						
LPR-0005	Optical Triggers	2		2	2	2	
LPR-0036	Sgl Lane Optical Trigger/Reflector assm w/stands	3		1	1	2	
LPR-0062	Dual Lane Optical Trigger PVC enclosure upgrade	1		2	2	2	
LPR-0045	P356 LPR 810nm camera w/5-50 varifocal lens, long hood	3		6	6	2	
Mobile LPI							

3M PARTS INVENTORY - JFK International Airport (Sept. 2015)

Part Number	Description	Required Stock Level	Maintenance Spares Breakdown				Notes
			Depot Repair	On Hand	Total	Re-Order	
Cashier Terminal, ACT, POF Gate Cabinet							
LP40000000000	SuperEx II Mobile	1		1	1	0	
PIPS-TSMIN	G-Net Monitor & Cables	1		1	1	0	
CA3620000000	SuperEx Camera Cable 15'	1		1	1	0	
P681W0806E00	P362 Cam W 810NM08IR06OV	1		1	1	0	

3M PARTS INVENTORY - Newark Liberty International Airport

Part Number	Description	Required Stock Level	Maintenance Spares On-Hand				Notes
			Depot Repair	On Hand	Total	Re-Order	
	Cashier Terminal, ACT, POF Gate Cabinet						
11-25202	ELO Touchscreen	4		5	5	2	
11-25180	CT Printer (Ithaca)	5	3	3	6	3	
11-25178	Check Combo Reader	4	1	8	9	2	
11-25224	Cash Drawer	4		7	7	2	
32-22361	TD400 Controller	10	2	20	22	5	
52-14056	Posi Drive Controller	10	12	24	36	5	
12-10424	Comm Gateway Controller	10		10	10	5	
31-12511	Printer Ribbon Cartridge, TD400	150		71	71	60	*Order for 150 requested from ABM*
32-22362	TD400 Field I/O Assembly	10		14	14	5	
32-22365	TD 420 Entrance Transport Assembly	10	8	9	17	5	
N/A	Retracted Ticket Bins	4		4	4	2	
32-22364	TD 420 Exit Transport Assembly	10	3	18	21	5	
30-25749	Ticket Deflector Plate	10		26	26		
32-22408	TD 420 POF Transport Assembly	6		6	6	3	
11-26377	POF Monitor	2		3	3	1	
11-25159	POF Credit Card Reader	4		3	3	2	
52-14053	LCD Display Interface	4		9	9	2	
82-20059	LCD - Display	4		9	9	2	
82-22383	ACT Receipt Printer (Patron)	4		15	15	2	
11-12262	Ultra Sonic Safety Sensor	0		1	1	2	*Obsolete*
51-25110	Gate Motors (Bodine DC Motor)	6	1	7	8	3	
50-25403	Main Spring Posi 50	20		31	31	10	
80-20491	Push for Ticket Buttons	4		2	2	2	
41-25652	Push for Receipt Buttons	4		3	3	2	
11-3914	Pushbutton Lightbulbs	10		1	1	5	*10 on order*
53-14001	Gate Drive Assembly	2		3	3	1	
11-25510	20 Amp Fuse Posi Drive Gate	20		26	26	10	*40 on order*
50-25072	Connecting Rod (Narrow)	10		0	0	5	*10 on order*
20-11903	Main Crank Shaft Pt 1 (Posidrive Gate)	4		3	3	2	
20-11920	Spring Crank (Posidrive Gate)	4		14	14	2	
20-11907	Motor Crank (Posidrive Gate)	5	5	1	6	3	*10 on order*
21-11921	Bearing Spring Crank	10		52	52	6	
21-11944	Posi Gate Switch (Posidrive Gate)[Door]	10	1	4	5	5	
12-10417	Universal Power Supply	2		12	12	1	
50-25112	Gate Arms 10ft	10	8	2	10	5	*10 on order*
50-25101	Gate Arm end cap	6		4	4	3	
62-15672	IP Dongles	10		13	13	5	
11-0003	T Handle lock w/key	5		4	4	3	
11-1743	5 Amp Fuse	20		20	20	10	
11-25159	Patron Credit Card Reader (ACT)	4	3	3	6	2	
41-17102	Power Supplies (ACT)	6	2	2	4	3	
11-25844	Pin pad (ACT)	4		9	9	2	
11-26099	16 Port Dlink Switch	5		5	5	3	
11-25027	Lock Assembly spitter doors	5		11	11	3	
11-25489	DB9 terminal adapter, 1 req'd per P357 trigger input	1		1	1	1	
11-25583	Floodlight fixture, dual	2		3	3	1	
11-25803	Sapphire, PANYNJ, configured w/sftwr & drivers	10	13	14	27	5	
11-25839	Novus 2 UPS w/extd alarm card	1		1	1	1	
11-11785	24VDC Fan	4		7	7	2	
12-10438	In-booth Mag Stripe Ticket Reader	4		4	4	2	
11-26185	Perle (Kapsch IV)	4		14	14	2	
800260-007	IAG-2T 007 Antenna (Kapsch IV)	1		1	1		
800260-008	IAG-2T 008 Antenna (Kapsch IV)	1		4	4		
12-25268	LPR/CCTV post w/L-bracket, U bolt, & (3) 4" caps	1		1	1	1	
52-14087	BRO-1 Buffer relay pkg (R/G light control)	2		8	8	1	
11-12238	HID MaxiProx Reader	3	1	3	4	2	
11-25879	Cisco Switch	3		4	4	2	
VMS-0019	VMS 1226-2 wall mtd 1.5" char. 2 line Red LED sign	4	1	9	10	2	
12-10451	DB9F to RJ45 adapter, 1 req'd per VMS	2		1	1	1	
12-10451	DB9-RJ12 Connector	2		35	35	1	
N/A	UPS Battery			60	60		*Replenished by ABM*
63-15713	II3 Intercom Assy	5		6	6	2	
12-10439	RB Intercom w/outdoor quad box	2		5	5	1	
	License Plate Recognition						
	CCTV Camera Domes	2		2	2	1	
CCTV-0004	Spectralite outdoor PTZ color camera	4	1	8	9	2	
CCTV-0006	Spectra outdoor wall pendant w/PS	6		4	4	3	
CCTV-0009	Video server, Axis 2400+	4		5	5	2	

3M PARTS INVENTORY - Newark Liberty International Airport

Part Number	Description	Required Stock Level	Maintenance Spares On-Hand				*Notes*
			Depot Repair	On Hand	Total	Re-Order	
Cashier Terminal, ACT, POF Gate Cabinet							
LPR-0001	P357 Image processor, PANYNJ ALPR Image Processor	4	4	5	9	2	
LPR-0004	LPR camera connector	1		1	1	1	
LPR-0005	Optical Triggers	0		2	2	6	*Obsolete*
LPR-0005	Optical Triggers	12		3	3	6	*6 on order will bring on-hand to 9 (New trigger replaced OT & Ultrasonic Sensor)*
LPR-0036	Sgl Lane Optical Trigger/Reflector assm w/stands	3		3	3	2	
LPR-0062	Dual Lane Optical Trigger PVC enclosure upgrade	4		6	6	2	
LPR-0045	P356 LPR 810nm camera w/5-50 varifocal lens, long hood	4		5	5	2	
Mobile LPI							
AP400000000000	SuperEx II Mobile	1		1	1	0	
PIPS-TSMIN	G-Net Monitor & Cables	1		1	1	0	
ACA362000000003	SuperEx Camera Cable 15'	1		1	1	0	
AP681W0806E000	P362 Cam W 810NM08IR06OV	1		1	1	0	

Parking Access and Revenue Control System—Design, Installation & Maintenance

Attachment T
EZ-Pass® ACH Requirements

Port Authority

Airport Central Host Requirements

For

04/29/2015
Version 5.5

1.0 Introduction

This document defines the unique specifications which will allow the PA to act as a Facility Operator (FO) as defined by the Reciprocity II agreement implemented by the IAG. This document must be used in conjunction with the E-ZPass IAG Facility Operator to Customer Service Center Interface File and Reporting Specifications document (FO-CSC Spec Version FO 1.51e).

General requirements include:

1. The Airport Central Host (ACH) shall be required to maintain at least 13 rolling months of detail transaction information on-line and will be expected to process 60,000 transactions daily.
2. The ACH shall be required to maintain at least 25 rolling months of summary information on-line.
3. The ACH database shall allow for ODBC connectivity.
4. A tape backup system shall be provided which allows for unattended system backups.
5. Only a single host is required at the Primary location.
6. A fully configured backup ACH is required to be installed at the Backup location. The database on the backup ACH shall be synchronized with the primary ACH via database replication or some other such method. While fully automated failover to the backup ACH is not required, failover processes shall be provided so as to minimize the time required for restoration of ACH services to the backup ACH to no more than 18 hours.

File interfaces required include:

File Type	Description
FO Tag Status File	Contains the list of valid tags. Sent from the CSC to the ACH.
FO Transaction File	Contains E-ZPass Plus transactions processed at the airports. Sent from the ACH to the CSC.
FO Distribution File	Contains information on the distribution of E-ZPass Plus transactions sent to each Home Agency/CSC. Sent from the CSC to the ACH.
FO Reconciliation File	Contains reconciliation information for a group of E-ZPass Plus transactions. Sent from the CSC to the ACH.
FO Correction File	Contains E-ZPass Plus transactions which are being re-submitted to the CSC for processing. Sent from the ACH to the CSC.

File Type	Description
FO Acknowledgement File	Contains acknowledgement information for files transferred between the ACH and the CSC.

The following sections go into detail on the various file level interfaces required on the ACH.

2.0 E-ZPass Plus Data Flow

The data flow between the Host CSC and the ACH is as follows:

1. On a nightly basis, the Host CSC creates an FO Tag Status File and transmits it to the ACH.
2. The ACH receives and processes the FO Tag Status File and transmits it down to the individual Airport Parking Hosts (APH). The ACH also creates an Acknowledgement File for the FO Tag Status File and transmits it to the Host CSC.
3. Throughout the day, the APHs collect/generate E-ZPass Plus transactions.
4. Periodically, but no less frequently than daily, the ACH retrieves the E-ZPass Plus transactions from the APHs and loads them into its database.
5. On a nightly basis, the ACH gathers the transactions loaded into its database, creates an FO Transaction File and transmits it to the Host CSC (assuming there were E-ZPass Plus transaction that day).
6. The Host CSC processes the FO Transaction File and transmits an Acknowledgement File and FO Distribution File to the ACH (typically within 48 hours of receipt of the FO Transaction File).
7. The ACH processes the Acknowledgement and Distribution Files and updates it database with the information found.
8. The Host CSC creates INTX files from the FO Transaction File and transmits them to their corresponding Home CSCs. Internally, the Host CSC creates INTX files for tags associated with its own accounts as well.
9. Each CSC, including the Host CSC, posts the E-ZPass Plus transactions valued at < $20 to the customer's accounts.
10. Each CSC, including the Host CSC, transmits the E-ZPass Plus transactions valued at >= $20 to the credit card processor.
11. The credit card processor responds to each transaction received indicating whether the transaction was authorized or declined.
12. If the transaction was declined by the credit card processor, the Home CSC flags the associated E-ZPass account as no longer participating in E-ZPass Plus and a letter is generated to the customer informing them that their credit card was declined.
13. The Home CSC creates an INRX file reconciling the data from the INTX file back to the Host CSC. The Host CSC creates an INRX file for the transactions processed against its own accounts as well.
14. For each INRX file received (including the ones the Host CSC generated), the Host CSC creates an FO Reconciliation File and transmits it to the ACH (typically with 4 to 5 days of receipt of the original FO Transaction File).

15. The ACH processes each FO Reconciliation File and updates its database with the information found.
16. Transactions which reconciled back with a code indicating that they were declined by the credit card processor (code of DECL) or with a code indicating that the E-ZPass account no longer has a credit card associated with it (code of NOCC) are kept in a holding queue on the ACH.
17. Because the E-ZPass account for declined transactions was flagged as no longer participating in E-ZPass Plus, the next FO Tag Status File transmitted by the Host CSC will not include any tags from that account.
18. On a daily basis, the ACH compares its holding queue to the latest FO Tag Status File. If a transaction in the holding queue has a tag that is found in the FO Tag Status File, it is an indication that the customer has put a new credit card on their E-ZPass account. Therefore, the ACH will take this transaction out of the holding queue and will include it in an FO Correction File for transmission to the Host CSC.
19. The FO Correction File is processed in the same manner as an FO Transaction File with corresponding FO Distribution Files, ITXN and IRXN Files and FO Correction Reconciliation Files.

    Per IAG guidelines, a transaction can only be resubmitted in an FO Correction File once. Therefore, if the transaction is rejected a second time as DECL or NOCC, the Facility Operator will not be able to pursue payment for the transaction from the Host CSC.
20. On a periodic basis (typically monthly), the Host Agency and the Facility Operator generate settlement reports (FO-1, FO-2, FO-3 and FO-4). The settlement reports indicate the funds due to the Facility Operator from the various Home Agencies via the Host Agency.

3.0 File Exchanges

3.1 FO Tag Status File (FTAG)

The CSC will transmit a tag file (FTAG) to the ACH via SFTP to a predetermined directory. This tag file will contain tags valid for E-ZPass Plus airport parking (TAG_STATUS = '1') as well as invalid tags (TAG_STATUS = '3') which are eligible for non-revenue discounts at PA airports based on the Discount bits shown below. The format of the file will follow the definition stipulated in the FO-CSC Spec for FO Tag Status Files.

The TAG_ACCT_INFO bits of the file shall be interpreted as follows:

FO Tag Status File - Detail Structure		
Field Name	**Type/Size**	**Description/Valid Values**
TAG_ACCT_INFO	CHAR(6)	A string of 24 bits (3 characters) converted to Hex-ASCII format (6 characters). The 24 bits represent the following: Bit 23 – 0: Discount bits 1 – Tag has associated discount plan 0 – Tag does not have associated plan Plan bits are defined as follows: Bit 0: PANYNJ Employee Non-revenue Bit 1: PANYNJ Annual Pass Non-revenue Bit 2: PANYNJ Vehicle Non-Revenue Bits 3 – 23: Reserved

The ACH will periodically check the predetermined directory for the CSC tag file and, when found, shall process the file using the ACH_CREATE_TAG_STATUS process. This process shall create a RCS Tag Status File for use by RCS (See Section **Error! Reference source not found.**, **Error! Reference source not found.**). The RCS Tag Status File shall contain information for both the valid and invalid tags presented in the FO Tag Status File including all discount information for both valid and invalid tags.

Appropriate sanity/reasonableness checking shall be used to ensure that invalid/corrupt FO Tag Status Files do not get processed and transmitted to the RCS servers.

This checking will include, but not be limited to:

1. The FTAG file name time matches the internal header time.
2. The FTAG header Agency ID is associated with an agency in the TR_HOST_AGENCY table.
3. The number of good tags declared in the header matches the number of total tags declared in the header
4. When given the command line option to check, we
    a) make sure the file processing is newer than the last one processed.
    b) make sure the declared count of "good tags" is between the shrinkage and growth bounds
5. The number of good tags in the FTAG file actually matches what was declared in the header.
6. Ensure that no invalid tags are in the FTAG file (other than those with non-revenue bits).

7. All tag agencies are in the TR_HOST_AGENCY table.
8. All tag numbers do not have non-numeric values.

The process shall accept a command line option to control whether or not the checking defined in (4) above shall be performed.

In addition, the process shall accept a command line option to control whether or not it shall update the ACH database with the information for the currently processed FTAG file.

This process shall produce a report showing its processing results. This report shall appear as follows:

```
Present Run Date/Time:  4-DEC-2000 10:39:02
   Last Run Date/Time:  3-DEC-2000 09:45:10


                         Port Authority of NY & NJ
                    E-ZPass Plus Create Tag Status File Report

               Processed Tag Status File: 008_20011109125326.FTAG
               Command Line:  ach_create_tag_status 008_20011109125326.FTAG DB_CHECK DETAIL ZIP


                                          Present Run      Last Run    %
Tag Status                                      #Tags         #Tags    Change
       1 - Valid                              4,626,697     4,638,103     -0.2%
       ? - Unknown                                    0             0      0.0%

Total Tags                                    4,626,697     4,638,103     -0.2%


Discount Flags
0 - Standard plan/no plan                     4,625,696
1 - Employee Non-Rev plan                             1
2 - Annual Pass Non-Rev plan                          0
3 - PA Vehicle Non-Rev plan                       1,000

Total Tags                                    4,626,697


-------------------------------------------------------------------------------
Agency                           Good   Unknown    Total
-------------------------------------------------------------------------------
004 (NYSTA)                   921,139         0     921,139

005 (PANYNJ)                  493,588         0     493,588

006 (PTC)                      26,693         0      26,693

008 (MTA B&T)               1,864,420         0   1,864,420

009 (DRPA)                    116,028         0     116,028

021 (Fast Lane, MassPike)     291,488         0     291,488

022 (Regional Consortium)     898,040         0     898,040

024 (WVPA)                     15,301         0      15,301

-------------------------------------------------------------------------------
```

Any errors detected during the processing of the file shall be indicated at the end of the report.

The report output shall be retained in a uniquely named file in a report directory on the ACH so that it can be retrieved by authorized staff for later review.

Appropriate log files shall be created to allow authorized staff to ascertain that the process ran successfully or, if the process failed, to determine the reason for said failure.

3.2 FO Transaction File

The ACH shall create a transaction file for the CSC using the CREATE_TRX_TO_CSC process. Format of the transaction file shall follow the definition stipulated in the FO-CSC Spec for FO Transaction Files. The transaction file shall be SFTPed by the ACH to a predetermined directory on the CSC system on at least a daily basis.

A set of transactions from a given RCS Transaction file cannot be split across multiple FO Transaction Files. In other words, all transactions for a given RCS TRAN_FILE_NUM must be sent in the same FO Transaction File. An FO Transaction File can contain transactions from multiple RCS Transaction Files.

This process shall produce a report showing its processing results. This report shall appear as follows:

```
Run Date/Time: 02-DEC-2000 08:00:30
                                        Port Authority of NY & NJ
                                 E-ZPass Plus CSC Transaction File Report


                                   FNTX   Record   Expected
Trans File Name                     Num    Count    Amount       Message

005_005_20001201075358.FNTX        12345      100   $2,000.00
```

The report columns are defined as follows:

Column Name	Description
Trans File Name	The name of the file created
FNTX Num	The unique serial number assigned to the file by the ACH
Record Count	The number of detail records in the file
Expected Amount	The total dollar value of all the detail records in the file
Message	Shows warning and error messages pertaining to the processing results of the file.

The report output shall be retained in a uniquely named file in a report directory on the ACH so that it can be retrieved by authorized staff for later review.

Appropriate log files shall be created to allow authorized staff to ascertain that the process ran successfully or, if the process failed, to determine the reason for said failure.

3.3 FO Distribution File

The CSC will transmit transaction and correction distribution data to the ACH via SFTP to a predetermined directory. Format of the distribution file will follow the definition stipulated in the FO-CSC Spec for FO Distribution Files.

The ACH shall periodically check this directory for distribution files and, when found, shall process all files found using the PROCESS_DISTRIB_FILE process, updating detail and summary tables as required.

This process shall produce a report showing its processing results. This report shall appear as follows:

```
Run Date/Time: 02-DEC-2000 08:00:30
```

```
                    Port Authority of NY & NJ
             E-ZPass Plus CSC Distribution File Report

                          Expect
                   FNTX   Record  Found   Home   INTX     Num       Expected
Distrib File Name   Num    Count  Record  Agcy    Num    Trans       Amount      Message

005_005_20001201075358.FNDX  12345       5      5     004   12345       39        $750.00
                                                      008   12346       45      $1,000.00
                                                      021   12347       10         $50.00
                                                      022   12358        5        $180.00
                                                      025   12360        1         $20.00
                                                                        --------  -------------
                                                                            100      $2,000.00
```

The report columns are defined as follows:

Column Name	Description
Distrib File Name	The name of the file being processed
FNTX Num	The unique serial number to which this file corresponds. This value is extracted from the header record of the file.
Expect Record Count	The number of records expected to be found in the file based on the header record of the file.
Found Record	The number of records actually found in the file.
Home Agcy	From the detail record
INTX Num	From the detail record
Num Trans	From the detail record
Expected Amount	From the detail record
Num Trans (total)	The sum of the “Num Trans” column for a single FNDX file.
Expected Amount (total)	The sum of the “Expected Amount” column for a single FNDX file.
Message	Shows warning and error messages pertaining to the processing results of the file. Possible messages include: Warning: FNTX mismatch - displayed when the totals of “Num Trans” and/or “Expected Amount” do not match the original FNTX file sent to the CSC. Warning: Unexpected EOF - displayed when “Found Record” does not equal “Expect Record Count” . Error: Could not update _____ table - displayed when there was a problem updating a detail or summary record. The actual table name is shown in the message.

The report output shall be retained in a uniquely named file in a report directory on the ACH so that it can be retrieved by authorized staff for later review.

Appropriate log files shall be created to allow authorized staff to ascertain that the process ran successfully or, if the process failed, to determine the reason for said failure.

3.4 FO Reconciliation File

The CSC will transmit transaction and correction reconciliation data to the ACH via SFTP to a predetermined directory. Format of the reconciliation file will follow the definition stipulated in the FO-CSC Spec for FO Reconciliation Files. The ACH shall periodically check this directory for the reconciliation files and, when found, shall process all files found using the PROCESS_RECON_FILE process, updating detail and summary tables as required.

This process shall produce a report showing its processing results. This report shall appear as follows:

```
Run Date/Time: 02-DEC-2000 08:00:30
                                    Port Authority of NY & NJ
                              E-ZPass Plus CSC Reconciliation Report

                                 Expect
                              INTX   Record  Found  Updated   Dupl.   Old  Inv
Recon File Name                Num    Count  Record  Record  Record   Rec  Rec  Message

022_005_20001201075358.FNRX   12358       5       5       5       0     0    0
021_005_20001201075358.FNRX   12347       9       9       9       0     0    0  Warning: FNDX mismatch
004_005_20001201075358.FNRX   12345      39      39      39       0     0    0
008_005_20001201075358.FNRX   12346      45      45      45       0     0    0
025_005_20001201075359.FNRX   12360       1       1       1       0     0    0
```

The report columns are defined as follows:

Column Name	Description
Recon File Name	The name of the file being processed
INTX Num	The index number assigned to the corresponding transaction file by the CSC
Expect Record Count	The number of records expected to be found in the file based on the header record of the file.
Found Record	The number of records actually found in the file.
Updated Record	The number of detail records updated
Dupl Record	The number of detail records not processed because they were duplicates of records already reconciled.
Old Rec	The number of detail records not processed because they had already been archived.
Inv Rec	The number of detail records not processed because they contained invalid data
Message	Shows warning and error messages pertaining to the processing results of the file. Possible messages include: Warning: File data is too old - displayed when the value in “Old Rec” is greater than zero. Warning: Unexpected EOF - displayed when “Found Record” does not equal “Expect Record Count” . Warning: FNDX mismatch - displayed when the number of records processed does not match that as indicated in the corresponding distribution record. Warning: Duplicate data - displayed when the value in “Dupl Rec” is greater than zero. Error: Could not update _____ table - displayed when there was a problem updating a detail or summary record. The actual table name is shown in the message.

The report output shall be retained in a uniquely named file in a report directory on the ACH so that it can be retrieved by authorized staff for later review.

Appropriate log files shall be created to allow authorized staff to ascertain that the process ran successfully or, if the process failed, to determine the reason for said failure.

3.5 FO Correction File

The ACH shall create a correction file for the CSC on an as needed basis. Format of the correction file shall follow the definition stipulated in the FO-CSC

Spec for FO Correction Files. The correction file shall be SFTPed by the ACH to a predetermined directory on the CSC system on at least a daily basis.

The correction file shall contain all parking transactions associated with E-ZPass Plus tags which have been flagged as corrected on the ACH since the last correction file was created for the CSC.

A process must be developed which allows E-ZPass Plus transactions to be corrected by a user via a workstation.

It will also contain all transactions which the ACH has determined can be resubmitted for posting to a customer account.

The ACH shall determine that a transaction is eligible for re-submittal as follows. All transactions reconciled by the CSC as not posted due to reject codes NOCC or DECL shall be examined on a daily basis. The tag information from these rejected transaction shall be compared to the most recent FO Tag Status File (received after the transaction date of the original rejected transaction) successfully processed by the ACH. If the tag is indicated as valid in the FO Tag Status File, the transaction shall be deemed as eligible for re-submittal to the CSC and shall be included in the next correction file.

A transaction can only be re-submitted for correction once. Also, a transaction can only be resubmitted for correction within 60 days of the original transaction date. Therefore, transaction older than 60 days cannot be corrected via a workstation, nor should they be part of the automatic correction process described above.

This process shall produce a report showing its processing results. This report shall appear as follows:

```
Run Date/Time: 02-DEC-2000 08:00:30
                                    Port Authority of NY & NJ
                               E-ZPass Plus CSC Correction File Report


                                 FTXN   Record   Expected
Correction File Name              Num    Count    Amount

005_005_20010501123456.FTXN      12345     100   $2,000.00
```

The report columns are defined as follows:

Column Name	Description
Correction File Name	The name of the file created
FTXN Num	The unique serial number assigned to the file by the ACH.
Record Count	The number of detail records in the file
Expected Amount	The total dollar value of all the detail records in the file

The report output shall be retained in a uniquely named file in a report directory on the ACH so that it can be retrieved by authorized staff for later review.

Appropriate log files shall be created to allow authorized staff to ascertain that the process ran successfully or, if the process failed, to determine the reason for said failure.

3.6 FO Acknowledgement File

The ACH shall create an FO Acknowledgement File for the CSC on an as needed basis. Format of the FO Acknowledgement File shall follow the definition stipulated in the FO-CSC Spec for FO Acknowledgement File. The FO Acknowledgement File shall be SFTPed by the ACH to a predetermined directory on the CSC system on at least a daily basis.

The CSC will transmit FO Acknowledgement Files to the ACH via SFTP to a predetermined directory. Format of the FO Acknowledgement File will follow the definition stipulated in the FO-CSC Spec for FO Acknowledgement Files. The ACH shall periodically check this directory for FO Acknowledgement File and, when found, shall process all files found using the PROCESS_ACK_FILE process, updating tables as required.

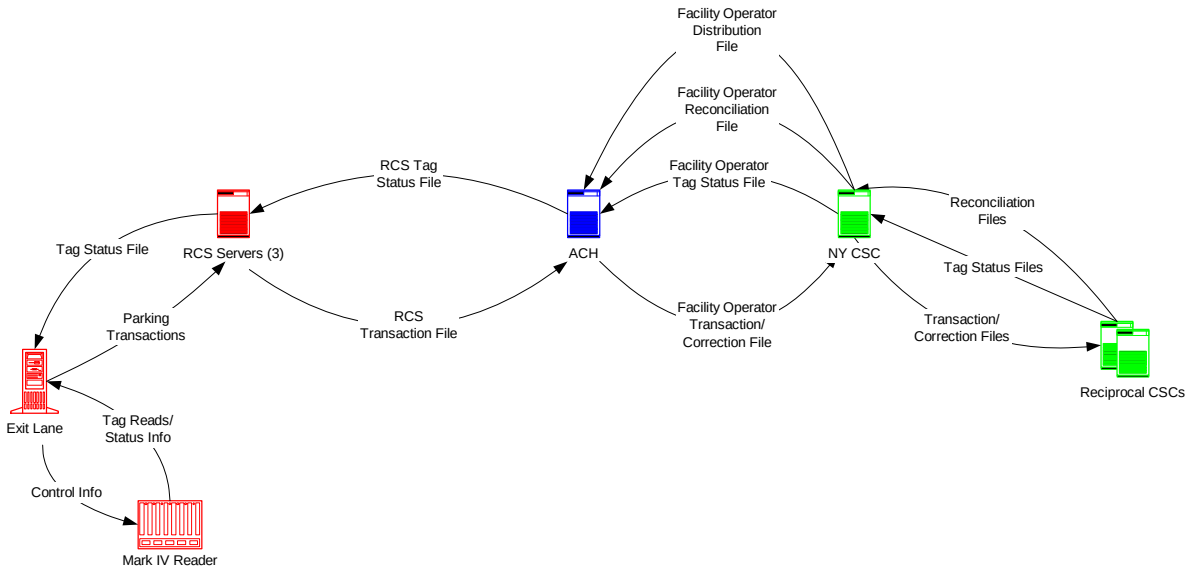
4.0 Graphical User Interface

The ACH shall provide a graphical user interface (GUI) which shall allow authorized user to perform the following functions:

- Edit the table of valid lanes
- Edit the table of valid plazas/locations
- Edit the table of authorized users/employees
- Edit the table which defines user roles on the system and screen permissions
- Correct transactions for resubmission to the CSC
- Run/View system reports

Access to the transaction correction function shall be restricted such that only users with access to the given facility/airport be allowed to correct transactions from the facility.

A. Dataflow Diagram Appendix



B. Additional Reports

The following reports must also be produced by the ACH on demand.

Report Number	Report Name
FO-1*	Facility Operator Period Transaction Summary Report
FO-2*	Facility Operator Period Correction Summary Report
FO-3*	Facility Operator Transaction Reconciliation Detail Report
FO-4*	Facility Operator Correction Reconciliation Detail Report
FO-3a	Facility Operator Transaction Reconciliation Detail Report - by Facility
FO-4a	Facility Operator Correction Reconciliation Detail Report - by Facility
ACH-0018	RCS Transaction Summary Report
ACH-0013	Revenue Reconciliation by Agency Report
ACH-0012	Open Transaction Summary Report
ACH-0011	Open Transaction Detail Report
ACH-0010	Eligible Resubmissions Summary Report
ACH-0009	Eligible Resubmissions Transaction Detail Report
ACH-0008	Declined Write-Off Summary Report
ACH-0007	Declined Write-Off Transaction Detail Report
ACH-0006	Tag File Report
ACH-0001	Employees Report
ACH-0002	Codes Report
ACH-0003	Lanes Report
ACH-0004	Locations Report
ACH-0005	Facilities Report
	CSC Transaction File Report
	CSC Distribution File Report
	CSC Reconciliation Report
	CSC Correction File Report

* Refer to the E-ZPass IAG Facility Operator to Customer Service Center Interface File and Reporting Specifications document (FO-CSC Spec Version FO 1.51e) for details on these reports.

FO-3a Facility Operator Transaction Reconciliation Detail Report - by Facility

Run Date: MM/DD/YYYY
Run Time: HH:MM
XXXXXXXXXXXXXX
Run By: X

Port Authority of NY & NJ - E-ZPass Plus System
Facility Operator Transaction Reconciliation Detail Report - by Facility
Transaction Reconciliation Files Acknowledged in:
Settlement Period: MM/DD/YYYY through MM/DD/YYYY

Page N of M
FO-3a

Facility: JFK
Home Agency: 022 - Regional Consortium

FNRX File	INRX Ack Date/Time	Total Trans	PSNT Count	PSNT Amount	DECL Count	DECL Amount	NOCC Count	NOCC Amount	Reject Count	Reject Amount
022_005_19990102010901.FNRX	mm/dd/yyy hh24:mi:ss	1,207	1,194	$ 35,503.10	3	$ 170.00	3	$ 30.00	7	$ 131.50
022_005_19990102010901.FNRX	mm/dd/yyy hh24:mi:ss	4,057	4,049	$ 89,100.00	2	$ 40.00	1	$ 10.00	5	$ 136.00
.										
.										
.										
022_005_19990102010901.FNRX	mm/dd/yyy hh24:mi:ss	850	846	$ 21,970.00	5	$ 200.00	3	$ 21.00	1	$ 45.00
Agency ### Total		6,114	6,089	$ 146,573.10	10	$ 410.00	7	$ 61.00	13	$ 312.50
Facility XXX Total		###,###	###,###	$#,###,###.##	###,###	$#,###,###.##	###,###	$#,###,###.##	###,###	$#,###,###.##
Report Total		###,###	###,###	$#,###,###.##	###,###	$#,###,###.##	###,###	$#,###,###.##	###,###	$#,###,###.##

Report Parameters:

Period start date — The user supplied start date (based on ACK file date) of the reporting period
Period end date — The user supplied end date (based on ACK file date) of the reporting period

Report Usage:

This report shows a summary breakdown of transaction reconciliation with the CSC by Facility and by Home Agency
The Report Total on this report should match that on the FO Tran Settlement report.

Field Definitions:

Run Date — Date the report is being executed

Run Time	The time the report is being executed
Run By	The user running the report
Settlement Period:	The period covered by the report
Facility	The facility (airport) for which the details apply
Home Agency	The IAG Code and name of the agency which owes the funds to the PA
FNRX File	The name of the transaction reconciliation file included in the settlement period
INRX Ack Date/Time	The date/time the INRX which corresponds to this FNRX file was acknowledged to the Home Agency Only FNRX files whose associated Ack date/time occurs during the Settlement Period are included in this report.
Total Trans	Total number of transactions reconciled in the file
PSNT Count	Total transactions reconciled with a code of PSNT in that file
PSNT Amount	Total dollar value of transactions with PSNT reconciliation code in the file
DECL Count	Total transactions reconciled with a code of DECL in that file
DECL Amount	Total dollar value (from original transactions) of transactions with DECL reconciliation code in that file
NOCC Count	Total transactions reconciled with a code of NOCC in that file
NOCC Amount	Total dollar value (from original transaction) of transactions with NOCC reconciliation code in that file
Reject Count	Total transactions reconciled with an other reject code in that file
Reject Amount	Total dollar value (from original transaction) of transactions with an other reject code in that file
Agency ### Total	Totals for the columns shown for that Home Agency for the Period where ### is the IAG Code of the Home Agency
Facility XXX Total	Totals for the columns shown for that Facility for the Period where XXX is the Facility abbreviation
Report Total	Totals for the columns shown for the Period

SAMPLE – FO-3a:

Port Authority of NY & NJ -E-ZPass Plus System

Report Date 04/29/2015

Time 15:55:39

Facility Operator Period Transaction Reconciliation Detail Report - by Facility

Report Number FO_3a

Settlement Period From: 01/01/2015 To: 01/31/2015

FNRX File	INRX ACK Date	Total Trans	PSNT Count	PSNT Amout	DECL Count	DECL Amout	NOCC Count	NOCC Amout	Reject Count	Reject Amout
Facility: EWR										
Home Agency: 004 - NYST										
004_131_20150101005714.FNRX	01/01/2015 00:57:14	194	192	$6,465.00	2	$288.00	0	$0.00	0	$0.00
004_131_20150102170020.FNRX	01/02/2015 17:00:20	191	189	$5,226.00	2	$40.00	0	$0.00	0	$0.00
004_131_20150103010028.FNRX	01/03/2015 01:00:28	182	181	$5,584.00	1	$24.00	0	$0.00	0	$0.00
004_131_20150103010038.FNRX	01/03/2015 01:00:38	229	228	$9,080.00	1	$33.00	0	$0.00	0	$0.00
004_131_20150104090042.FNRX	01/04/2015 09:00:42	130	128	$5,825.00	2	$149.00	0	$0.00	0	$0.00
004_131_20150106020017.FNRX	01/06/2015 02:00:17	150	149	$6,593.00	1	$102.00	0	$0.00	0	$0.00
004_131_20150106020022.FNRX	01/06/2015 02:00:22	221	220	$8,573.00	1	$33.00	0	$0.00	0	$0.00
004_131_20150107020019.FNRX	01/07/2015 02:00:19	210	207	$7,670.00	3	$654.00	0	$0.00	0	$0.00
004_131_20150110020019.FNRX	01/10/2015 02:00:19	176	175	$6,086.00	1	$132.00	0	$0.00	0	$0.00
004_131_20150113000021.FNRX	01/13/2015 00:00:21	159	158	$4,597.00	0	$0.00	1	$20.00	0	$0.00
004_131_20150113110009.FNRX	01/13/2015 11:00:09	249	248	$8,721.00	1	$150.00	0	$0.00	0	$0.00
004_131_20150114020015.FNRX	01/14/2015 02:00:15	180	178	$3,543.00	1	$32.00	1	$20.00	0	$0.00
004_131_20150114020023.FNRX	01/14/2015 02:00:23	179	178	$5,813.00	1	$32.00	0	$0.00	0	$0.00
004_131_20150115010025.FNRX	01/15/2015 01:00:25	160	160	$5,315.00	0	$0.00	0	$0.00	0	$0.00
004_131_20150115010028.FNRX	01/15/2015 01:00:28	174	174	$4,665.00	0	$0.00	0	$0.00	0	$0.00
004_131_20150115010030.FNRX	01/15/2015 01:00:30	197	195	$6,001.00	2	$123.00	0	$0.00	0	$0.00
004_131_20150118110007.FNRX	01/18/2015 11:00:07	139	137	$4,524.00	2	$375.00	0	$0.00	0	$0.00
004_131_20150118110011.FNRX	01/18/2015 11:00:11	142	142	$4,037.00	0	$0.00	0	$0.00	0	$0.00
004_131_20150118110014.FNRX	01/18/2015 11:00:14	155	154	$5,339.00	1	$33.00	0	$0.00	0	$0.00
004_131_20150119020015.FNRX	01/19/2015 02:00:15	176	173	$6,165.00	3	$336.00	0	$0.00	0	$0.00
004_131_20150119020021.FNRX	01/19/2015 02:00:21	173	172	$5,661.00	1	$20.00	0	$0.00	0	$0.00
004_131_20150121170011.FNRX	01/21/2015 17:00:11	183	183	$7,529.00	0	$0.00	0	$0.00	0	$0.00
004_131_20150121180010.FNRX	01/21/2015 18:00:10	173	168	$7,042.00	4	$633.00	1	$48.00	0	$0.00
004_131_20150122110012.FNRX	01/22/2015 11:00:12	189	186	$7,475.00	3	$207.00	0	$0.00	0	$0.00
004_131_20150123010012.FNRX	01/23/2015 01:00:12	125	123	$3,918.00	2	$270.00	0	$0.00	0	$0.00
004_131_20150124020011.FNRX	01/24/2015 02:00:11	130	129	$5,033.00	1	$189.00	0	$0.00	0	$0.00

FO-4a **Facility Operator Correction Reconciliation Detail Report - by Facility**

Run Date:	MM/DD/YYYY	Port Authority of NY & NJ - E-ZPass Plus System	Page N of M
Run Time:	HH:MM	Facility Operator Correction Reconciliation Detail Report - by Facility	FO-4a
Run By:	XXXXXXXXXXXXXXX	Correction Reconciliation Files Acknowledged in:	
		Settlement Period: MM/DD/YYYY through MM/DD/YYYY	

Facility: JFK
Home Agency: 022 - Regional Consortium

FRXN_FILE	IRXN Ack Date/Time	Total Trans	PSNT Count	PSNT ORG	PSNT NEW	PSNT NET	Final Reject Count	Final Reject Amount
022_131_19990102010901.FRXN	mm/dd/yyyy hh24:mi:ss	5	###,###	$ 24.00	$ 35.00	$ 11.00	0	$ -
022_131_19990105012448.FRXN	mm/dd/yyyy hh24:mi:ss	4	###,###	$ 10.00	$ 8.00	$ (2.00)	1	$ 3.00
022_131_19990106011057.FRXN	mm/dd/yyyy hh24:mi:ss	100	###,###	$ 825.00	$ 975.00	$ 150.00	0	$ -
Agency ### Total		###,###	###,###	$###,###.##	$###,###.##	$###,###.##	###,###	$###,###.##
Facility XXX Total		###,###	###,###	$###,###.##	$###,###.##	$###,###.##	###,###	$###,###.##
Report Total		109	###,###			$ 159.00	1	$ 3.00

Report Parameters:

Period start date	The user supplied start date (based on ACK file date) of the reporting period
Period end date	The user supplied end date (based on ACK file date) of the reporting period

Report Usage:

This report shows a summary breakdown of correction reconciliation with the CSC by Facility and by Home Agency.
The Report Total on this report should match that on the FO Corr Settlement report.

Field Definitions:

Run Date	Date the report is being executed
Run Time	The time the report is being executed
Run By	The user running the report
Settlement Period:	The period covered by the report
Facility	The facility (airport) for which the details apply
Home Agency	The IAG Code and name of the agency which owes the funds to the PA

FRXN File	The name of the correction reconciliation file included in the settlement period
INRX Ack Date/Time	The date/time the IRXN which corresponds to this FRXN file was acknowledged to the Home Agency Only FRXN files whose associated Ack date/time occurs during the Settlement Period are included in this report.
Total Trans	Total number of corrections reconciled in the file
PSNT Count	Total corrections reconciled with a code of PSNT in that file
PSNT ORG	Total original dollar value of transactions with PSNT reconciliation code in the file
PSNT NEW	Total new dollar value of transactions with PSNT reconciliation code in the file
PSNT NET	Total net difference between the original and new dollar value of transactions with PSNT reconciliation code in the file
Final Reject Count	Total corrections reconciled with any reject code in that file
Final Reject Amount	Total dollar value (from original transaction) of corrections with any reject code in that file
Agency ### Total	Totals for the columns shown for that Home Agency for the Period where ### is the IAG Code of the Home Agency
Facility XXX Total	Totals for the columns shown for that Facility for the Period where XXX is the Facility abbreviation
Report Total	Totals for the columns shown for the Period

SAMPLE – FO-4a:

Report Date 04/29/2015
Time 16:01:41

Port Authority of NY & NJ - E-ZPass Plus System
Facility Operator Correction Reconciliation Detail Report - by Facility
Correction ReconciliationFiles Acknowledged in:
Settlement Period: 01/01/2015 through 01/31/2015

Report Number FO_4a

FRXN_File	IRXN Ack Date/	Total Trans	PSNT Count	ORG	PSNT NEW	NET	Final Reject Count	Final Reject Amout
Facility: EWR								
Home Agency: 004 - NYST								
004_131_20150102150036.FRXN	01/02/2015 15:00:36	2	2	$0.00	$47.00	$47.00	0	$0.00
004_131_20150104224455.FRXN	01/04/2015 22:44:55	2	2	$0.00	$120.00	$120.00	0	$0.00
004_131_20150105010041.FRXN	01/05/2015 01:00:41	1	1	$0.00	$20.00	$20.00	0	$0.00
004_131_20150105194858.FRXN	01/05/2015 19:48:58	4	4	$0.00	$199.00	$199.00	0	$0.00
004_131_20150106010039.FRXN	01/06/2015 01:00:39	3	3	$0.00	$472.00	$472.00	0	$0.00
004_131_20150107010050.FRXN	01/07/2015 01:00:50	2	2	$0.00	$40.00	$40.00	0	$0.00
004_131_20150110020021.FRXN	01/10/2015 02:00:21	2	2	$0.00	$215.00	$215.00	0	$0.00
004_131_20150113000026.FRXN	01/13/2015 00:00:26	1	1	$0.00	$330.00	$330.00	0	$0.00
004_131_20150113000041.FRXN	01/13/2015 00:00:41	2	2	$0.00	$135.00	$135.00	0	$0.00
004_131_20150113000053.FRXN	01/13/2015 00:00:53	1	1	$0.00	$156.00	$156.00	0	$0.00
004_131_20150114020029.FRXN	01/14/2015 02:00:29	2	2	$0.00	$363.00	$363.00	0	$0.00
004_131_20150116010043.FRXN	01/16/2015 01:00:43	3	3	$0.00	$383.00	$383.00	0	$0.00
004_131_20150118110009.FRXN	01/18/2015 11:00:09	1	1	$0.00	$99.00	$99.00	0	$0.00
004_131_20150118110016.FRXN	01/18/2015 11:00:16	1	1	$0.00	$20.00	$20.00	0	$0.00
004_131_20150118110023.FRXN	01/18/2015 11:00:23	2	2	$0.00	$164.00	$164.00	0	$0.00
004_131_20150121180014.FRXN	01/21/2015 18:00:14	3	3	$0.00	$291.00	$291.00	0	$0.00
004_131_20150122110015.FRXN	01/22/2015 11:00:15	1	1	$0.00	$108.00	$108.00	0	$0.00
004_131_20150123010015.FRXN	01/23/2015 01:00:15	2	2	$0.00	$354.00	$354.00	0	$0.00
004_131_20150124010019.FRXN	01/24/2015 01:00:19	1	1	$0.00	$61.00	$61.00	0	$0.00
004_131_20150125010014.FRXN	01/25/2015 01:00:14	2	2	$0.00	$450.00	$450.00	0	$0.00
004_131_20150127020009.FRXN	01/27/2015 02:00:09	4	4	$0.00	$393.00	$393.00	0	$0.00
004_131_20150130010029.FRXN	01/30/2015 01:00:29	1	1	$0.00	$108.00	$108.00	0	$0.00

ACH-0018 RCS Transaction Summary Report

Run Date: MM/DD/YYYY
Run Time: HH:MM
Run By: XXXXXXXXXXXXXXX

Port Authority of NY & NJ - E-ZPass Plus System
RCS Transaction Summary Report

Page N of M
ACH-0018

Period: MM/DD/YYYY through MM/DD/YYYY

Revenue Date	EWR		JFK		LGA		Date Total	
MM/DD/YYYY	###,###	$#,###,###.##	###,###	$#,###,###.##	###,###	$#,###,###.##	###,###	$#,###,###.##
.	.		.		.		.	
.	.		.		.		.	
.	.		.		.		.	
.	.		.		.		.	
.	.		.		.		.	
.	.		.		.		.	
.	.		.		.		.	
Report Totals	###,###	$#,###,###.##	###,###	$#,###,###.##	###,###	$#,###,###.##	###,###	$#,###,###.##

Report Parameters:

Period start date	The user supplied start date (based on revenue date, not transaction date) of the reporting period
Period end date	The user supplied end date (based on revenue date, not transaction date) of the reporting period

Report Usage:

This report shows a summary breakdown of the number of E-ZPass Plus transactions received from RCS

Field Definitions:

Run Date	Date the report is being executed
Run Time	The time the report is being executed
Run By	The user running the report
Period:	The period covered by the report
Revenue Date	The revenue date of the summary data
EWR	The number and expected dollar amount of open E-ZPass Plus transactions for EWR for the given summary date
JFK	The number and expected dollar amount of open E-ZPass Plus transactions for JFK for the given summary date

LGA	The number and expected dollar amount of open E-ZPass Plus transactions for LGA for the given summary date
Date Total	The total number of open E-ZPass Plus transactions (and expected dollar amounts) for the given summary date
Report Totals	Totals for the columns shown for the Period

NOTE:
This report shall also be available by RCS transmission file number where the reporting period would be a from and to file number and the summaries would be by file number instead of by date.

SAMPLE – ACH-0018:

Port Authority of NY & NJ - E-ZPass Plau System

RCS Transaction Summary Report

Report Date 04/29/2015
Time 15:05:24

Reporting Period From: 01/01/2015 To: 01/31/2015

Report Number ACH0018

Revenue Date	Trans Recieved		Accepted		Rejected	
	Count	Amount	Count	Amount	Count	Amount
Facility: EWR						
01/01/2015	2305	$70,720.00	2305	$70,720.00	0	$0.00
01/02/2015	3043	$99,838.00	3043	$99,838.00	0	$0.00
01/03/2015	3370	$105,168.00	3370	$105,168.00	0	$0.00
01/04/2015	3950	$112,102.00	3950	$112,102.00	0	$0.00
01/05/2015	3238	$80,850.00	3238	$80,850.00	0	$0.00
01/06/2015	2766	$56,057.00	2766	$56,057.00	0	$0.00
01/07/2015	2671	$54,700.00	2671	$54,700.00	0	$0.00
01/08/2015	3102	$67,933.00	3102	$67,933.00	0	$0.00
01/09/2015	3239	$77,890.00	3239	$77,890.00	0	$0.00
01/10/2015	2710	$54,248.00	2710	$54,248.00	0	$0.00
01/11/2015	3464	$84,422.00	3464	$84,422.00	0	$0.00
01/12/2015	2817	$66,366.00	2817	$66,366.00	0	$0.00
01/13/2015	2586	$56,396.00	2586	$56,396.00	0	$0.00
01/14/2015	2883	$65,308.00	2883	$65,308.00	0	$0.00
01/15/2015	3524	$79,460.00	3524	$79,460.00	0	$0.00
01/16/2015	3605	$86,057.00	3605	$86,057.00	0	$0.00
01/17/2015	2568	$53,020.00	2568	$53,020.00	0	$0.00
01/18/2015	2839	$83,808.00	2839	$83,808.00	0	$0.00

ACH-0013 Revenue Reconciliation by Agency Report

Run Date: MM/DD/YYYY
Run Time: HH:MM
Run By: XXXXXXXXXXXXXXX

Port Authority of NY & NJ - E-ZPass Plus System
Revenue Reconciliation Summary by Agency Report

Page N of M
ACH-0013

Period: MM/DD/YYYY through MM/DD/YYYY
Facility: XXX

		Total		PSNT		DECL/NOCC		REJ	
Revenue Date	Home Agency	# Trans	Amount	# Trans	Amount	# Trans	Amount	# Trans	Amount
MM/DD/YYYY	XXXXXXXXX	###,###	$###,###.##	###,###	$###,###.##	###,###	$###,###.##	###,###	$###,###.##
.		.	.						
.		.	.						
Date Totals		###,###	$###,###.##	###,###	$###,###.##	###,###	$###,###.##	###,###	$###,###.##
.		.	.						
.		.	.						
.		.	.						
.		.	.						
Report Totals		###,###	$#,###,###.##	###,###	$#,###,###.##	###,###	$#,###,###.##	###,###	$#,###,###.##

Report Parameters:

Period start date	The user supplied start date (based on revenue date, not transaction date) of the reporting period
Period end date	The user supplied end date (based on revenue date, not transaction date) of the reporting period
Facility	The airport to be reported on. Can be a single facility or ALL to combine all in a single page.

Report Usage:

This report shows a summary breakdown of the number of E-ZPass Plus transactions and their associated revenue that has been processed and reconciled by the CSC..

Field Definitions:

Run Date	Date the report is being executed
Run Time	The time the report is being executed
Run By	The user running the report
Period:	The period covered by the report

Facility:	The facility represented in the report or ALL if all are combined
Revenue Date	The revenue date of the summary data
Home Agency	The Home Agency to whom the transactions were sent.
Total	Total number of transactions and associated amount
PSNT	The number/value of posted transactions
DECL/NOCC	The number/value of declined/no credit card transactions
REJ	The number/value of rejected transactions
Date Totals	Totals for the columns shown for the Date/File
Report Totals	Totals for the columns shown for the Period

SAMPLE – ACH-0013:

Port Authority of NY & NJ - E-ZPass Plus System

Revenue Reconciliation Summary By Agency Report

Report Date 04/29/2015

Time 14:55:09

Reporting Period From: 01/01/2015 To: 01/31/2015

Report Number ACH 0013

Revenue Date	Home Agency	DECL / NOCC Count	DECL / NOCC Amount	PSNT Count	PSNT Amount	RJCT Count	RJCT Amount	Total Processed Count	Total Processed Amount
Facility : EWR									
01/01/2015	DDOT	0	$0.00	4	$65.00	0	$0.00	4	$65.00
01/01/2015	DRJT	0	$0.00	15	$202.00	0	$0.00	15	$202.00
01/01/2015	MTA	0	$0.00	449	$14,589.00	0	$0.00	449	$14,589.00
01/01/2015	MdTA	0	$0.00	4	$286.00	0	$0.00	4	$286.00
01/01/2015	NHDT	0	$0.00	1	$78.00	0	$0.00	1	$78.00
01/01/2015	NJ	0	$0.00	1,174	$33,498.00	4	$728.00	1,178	$34,226.00
01/01/2015	NYST	0	$0.00	150	$6,695.00	0	$0.00	150	$6,695.00
01/01/2015	PA	0	$0.00	445	$13,147.00	1	$189.00	446	$13,336.00
01/01/2015	PTC	0	$0.00	57	$1,078.00	1	$165.00	58	$1,243.00
Total For Revenue Date 01/01/2015		0	$0.00	2,299	$69,638.00	6	$1,082.00	2,305	$70,720.00
01/02/2015	DDOT	0	$0.00	12	$168.00	0	$0.00	12	$168.00
01/02/2015	DRBA	0	$0.00	2	$20.00	0	$0.00	2	$20.00
01/02/2015	DRJT	0	$0.00	22	$512.00	0	$0.00	22	$512.00
01/02/2015	MTA	0	$0.00	621	$21,404.00	0	$0.00	621	$21,404.00
01/02/2015	MdTA	0	$0.00	9	$112.00	0	$0.00	9	$112.00
01/02/2015	NHDT	0	$0.00	3	$57.00	1	$132.00	4	$189.00
01/02/2015	NJ	0	$0.00	1,462	$47,404.00	4	$816.00	1,466	$48,220.00
01/02/2015	NYST	0	$0.00	220	$8,573.00	1	$33.00	221	$8,606.00
01/02/2015	PA	0	$0.00	628	$18,944.00	0	$0.00	628	$18,944.00
01/02/2015	PTC	0	$0.00	57	$1,643.00	1	$20.00	58	$1,663.00
Total For Revenue Date 01/02/2015		0	$0.00	3,036	$98,837.00	7	$1,001.00	3,043	$99,838.00
01/03/2015	DDOT	0	$0.00	12	$148.00	0	$0.00	12	$148.00
01/03/2015	DRBA	0	$0.00	1	$12.00	0	$0.00	1	$12.00
01/03/2015	DRJT	0	$0.00	29	$1,426.00	0	$0.00	29	$1,426.00
01/03/2015	MTA	0	$0.00	711	$22,155.00	1	$20.00	712	$22,175.00

ACH-0012 Open Transaction Summary Report

Run Date: MM/DD/YYYY
Run Time: HH:MM
Run By: XXXXXXXXXXXXXXX

Port Authority of NY & NJ - E-ZPass Plus System
Open (Unreconciled) Transaction Summary Report

Page N of M
ACH-0012

Period: MM/DD/YYYY through MM/DD/YYYY

Revenue Date	EWR		JFK		LGA		Date Total	
MM/DD/YYYY	###,###	$#,###,###.##	###,###	$#,###,###.##	###,###	$#,###,###.##	###,###	$#,###,###.##
.	.		.		.		.	
.	.		.		.		.	
.	.		.		.		.	
.	.		.		.		.	
.	.		.		.		.	
.	.		.		.		.	
.	.		.		.		.	
Report Totals	###,###	$#,###,###.##	###,###	$#,###,###.##	###,###	$#,###,###.##	###,###	$#,###,###.##

Report Parameters:

Period start date	The user supplied start date (based on revenue date, not transaction date) of the reporting period
Period end date	The user supplied end date (based on revenue date, not transaction date) of the reporting period

Report Usage:

This report shows a summary breakdown of the number of E-ZPass Plus transactions sent to the CSC that have not yet been reconciled back to the ACH.

Field Definitions:

Run Date	Date the report is being executed
Run Time	The time the report is being executed
Run By	The user running the report
Period:	The period covered by the report
Revenue Date	The revenue date of the summary data
EWR	The number and expected dollar amount of open E-ZPass Plus transactions for EWR for the given summary date
JFK	The number and expected dollar amount of open E-ZPass Plus transactions for JFK for the given summary date

LGA	The number and expected dollar amount of open E-ZPass Plus transactions for LGA for the given summary date
Date Total	The total number of open E-ZPass Plus transactions (and expected dollar amounts) for the given summary date
Report Totals	Totals for the columns shown for the Period

NOTE:
This report shall also be available by transmission file number (FNTX or FTXN) where the reporting period would be a from and to file number and the summaries would be by file number instead of by date.

SAMPLE – ACH-0012:

Port Authority of NY & NJ - E-ZPass Plus System

Report Date 04/29/2015

Time 14:52:22

Open (Unreconciled) Transaction Summary Report

Reporting Period From: 04/01/2015 To: 04/07/2015

Report Number ACH 0012

	EWR		JFK		LGA		Total	
Revenue Date	**Count**	**Amount**	**Count**	**Amount**	**Count**	**Amount**	**Count**	**Amount**
04/01/2015	0	$0.00	0	$0.00	1	$55.00	1	$55.00
04/02/2015	0	$0.00	0	$0.00	0	$0.00	0	$0.00
04/03/2015	0	$0.00	2	$40.00	0	$0.00	2	$40.00
04/04/2015	1	$180.00	0	$0.00	0	$0.00	1	$180.00
04/05/2015	0	$0.00	1	$102.00	0	$0.00	1	$102.00
04/06/2015	2	$156.00	1	$20.00	0	$0.00	3	$176.00
04/07/2015	1	$296.00	1	$165.00	0	$0.00	2	$461.00
Total For Revenue Dates Between 04/01/2015 And 04/07/2015								
	4	$632.00	5	$327.00	1	$55.00	10	$1,014.00

ACH-0011 Open Transaction Detail Report

Run Date:	MM/DD/YYYY	Port Authority of NY & NJ - E-ZPass Plus System	Page N of M
Run Time:	HH:MM	Open (Unreconciled) Transaction Detail Report	ACH-0011
Run By:	XXXXXXXXXXXXXXX		

Period: MM/DD/YYYY through MM/DD/YYYY

Facility: XXX Plaza/Lane: XXXXX

Revenue Date	Facility	Exit Plaza/Lane	Exit Date/Time	Entry Date/Time	Entry Plaza/Lane	Tag #	Pgm Stat	Lane Mode	Amout Due	RCS File	FNTX File	FTXN File
MM/DD/YYYY	XXX	PPPP/LLLL	MM/DD/YYYY HH:MM:SS	MM/DD/YYYY HH:MM:SS	PPPP/LLLL	###-#######	X	XXXXX	$###,###.##	#########	#########	#########
.	.	.	.	.	.	.						
.	.	.	.	.	.	.						
.	.	.	.	.	.	.						
.	.	.	.	.	.	.						
.	.	.	.	.	.	.						
.	.	.	.	.	.	.						
.	.	.	.	.	.	.						

Report Parameters:

Period start date	The user supplied start date (based on revenue date) of the reporting period
Period end date	The user supplied end date (based on revenue date) of the reporting period
Facility:	The user supplied airport to be reported on or ALL for all airports
Plaza/Lane:	The user supplied airport plaza/lane to be reported on or ALL for all plazas/lanes at the selected airport

Report Usage:

This report shows details of E-ZPass Plus transactions sent to the CSC that have not yet been reconciled back to the ACH.

Field Definitions:

Run Date	Date the report is being executed
Run Time	The time the report is being executed
Run By	The user running the report
Period:	The period covered by the report

Facility:	The facility represented in the report or ALL if all are combined
Plaza/Lane:	The plaza/lane represented in the report of ALL
Revenue Date	The revenue date of the transaction
Facility	The facility of the transaction
Plaza/Lane	The plaza/lane of the transaction
Exit Date/Time	The exit date/time of the transaction
Tran Serial	The transaction detail serial number
Entry Date/Time	The entry date/time of the transactions
Tag #	The tag agency/serial number associated with the transaction
Pgm Stat	The tag program status
Lane Mode	The operating mode of the lane at the time of the transaction
Amount Due	The amount due for the transaction
RCS File	The number of the RCS file in which this transaction was received from RCS
FNTX File	The number of the FNTX file in which this transaction was sent to the CSC
FTXN File	The number of the FTXN file (correction file) in which this transaction was sent to the CSC

SAMPLE – ACH-0011:

Port Authority of NY & NJ - E-ZPass Plus System

Report Date 04/29/2015

Time 14:50:41

Open (Unreconciled) Transaction Detail Report

Reporting Period From: 04/01/2015 To: 04/07/2015

Report Number ACH 0011

Exit Date/Time	Entry Date/Time	Entry Plaza	Entry Lane	Tag #	Pgm Stats	Lane Mode	Amt. Due	RCS File	FNTX File	FTXN File
Revenue Date: 04/01/2015										
Facility : LGA Airport										
Exit Location : Lot 6										
Exit Lane : 601										
04/01/2015 17:45:03	03/31/2015 16:02:37	LL6	602	008-08401166	S	E	$55.00	031946	104879	104421
Total Amount Due For Exit Lane : 601					Count	1	$55.00			
Total Amount Due For Exit Location : Lot 6					Count	1	$55.00			
Total Amount Due For Facility : LGA Airport					Count	1	$55.00			
Total Amount Due For Revenue Date: 04/01/2015					Count	1	$55.00			

ACH-0010 Eligible Resubmissions Summary Report

Run Date: MM/DD/YYYY
Run Time: HH:MM
Run By: XXXXXXXXXXXXXXX

Port Authority of NY & NJ - E-ZPass Plus System
Eligible Resubmissions Summary Report

Page N of M
ACH-0010

Period: MM/DD/YYYY through MM/DD/YYYY

Revenue Date	EWR		JFK		LGA		Date Total	
	# Trans	Amount	# Trans	Amount	# Trans	Amount	# Trans	Amount
MM/DD/YYYY	###,###	$###,###.##	###,###	$###,###.##	###,###	$###,###.##	###,###	$###,###.##
.	.		.		.		.	
.	.		.		.		.	
.	.		.		.		.	
.	.		.		.		.	
.	.		.		.		.	
.	.		.		.		.	
Report Totals	###,###	$#,###,###.##	###,###	$#,###,###.##	###,###	$#,###,###.##	###,###	$#,###,###.##

Report Parameters:

Period start date	The user supplied start date (based on revenue date) of the reporting period
Period end date	The user supplied end date (based on revenue date) of the reporting period

Report Usage:

This report shows a summary breakdown of the number of E-ZPass Plus transactions which were reconciled by the CSC as DECL or NOCC and are eligible for resubmission via the corrections file if a new tag status file were to indicate that the tag is again eligible for E-ZPass Plus.

Field Definitions:

Run Date	Date the report is being executed
Run Time	The time the report is being executed
Run By	The user running the report
Period:	The period covered by the report
Revenue Date	The revenue date of the summary data
EWR	The number/value of eligible E-ZPass Plus transactions for EWR for the given summary date

JFK	The number/value of eligible E-ZPass Plus transactions for JFK for the given summary date
LGA	The number/value of eligible E-ZPass Plus transactions for LGA for the given summary date
Date Total	The total number/value of eligible E-ZPass Plus transactions for the given summary date
Report Totals	Totals for the columns shown for the Period

SAMPLE – ACH-0010:

Port Authority of NY & NJ - E-ZPass Plus System

Report Date 04/29/2015

Eligible Resubmissions Summary Report

Report Number ACH 0010

Time 14:49:20

Reporting Period From: 04/01/2015 To: 04/07/2015

	EWR		JFK		LGA		Total	
Revenue Date	**Count**	**Amount**	**Count**	**Amount**	**Count**	**Amount**	**Count**	**Amount**
04/01/2015	7	$450.00	17	$868.00	2	$186.00	26	$1,504.00
04/02/2015	11	$542.00	10	$749.00	3	$246.00	24	$1,537.00
04/03/2015	10	$783.00	19	$988.00	2	$348.00	31	$2,119.00
04/04/2015	6	$645.00	22	$1,542.00	3	$375.00	31	$2,562.00
04/05/2015	4	$459.00	12	$874.00	4	$541.00	20	$1,874.00
04/06/2015	7	$479.00	10	$1,365.00	10	$1,461.00	27	$3,305.00
04/07/2015	8	$593.00	8	$265.00	3	$429.00	19	$1,287.00
Total For Revenue Dates Between 04/01/2015 And 04/07/2015								
	53	$3,951.00	98	$6,651.00	27	$3,586.00	178	$14,188.00

ACH-0009 Eligible Resubmissions Transaction Detail Report

Run Date:	MM/DD/YYYY	Port Authority of NY & NJ - E-ZPass Plus System	Page N of M
Run Time:	HH:MM	Eligible Resubmissions Transaction Detail Report	ACH-0009
Run By:	XXXXXXXXXXXXXXX		

Period: MM/DD/YYYY through MM/DD/YYYY

Facility: XXX Plaza/Lane: XXXXX

Revenue Date	Facility	Exit Plaza/Lane	Exit Date/Time	Entry Date/Time	Entry Plaza/Lane	Tag #	Pgm Stat	Lane Mode	Amout Due	RCS File	FNTX File	Recon Stat
MM/DD/YYYY	XXX	PPPP/LLLL	MM/DD/YYYY HH:MM:SS	MM/DD/YYYY HH:MM:SS	PPPP/LLLL	###-#######	X	XXXXX	$###,###.##	#########	#########	XXXX
.	.	.	.	.								
.	.	.	.	.								
.	.	.	.	.								
.	.	.	.	.								

Report Parameters:

Period start date	The user supplied start date (based on revenue date) of the reporting period
Period end date	The user supplied end date (based on revenue date) of the reporting period
Facility:	The user supplied airport to be reported on or ALL for all airports
Plaza/Lane:	The user supplied airport plaza/lane to be reported on or ALL for all plazas/lanes at the selected airport

Report Usage:

This report shows details of E-ZPass Plus transactions sent to the CSC that

have been reconciled back as DECL or NOCC and are still eligible for resubmission

Field Definitions:

Run Date	Date the report is being executed
Run Time	The time the report is being executed
Run By	The user running the report
Period:	The period covered by the report
Facility:	The facility represented in the report or ALL if all are combined
Plaza/Lane:	The plaza/lane represented in the report of ALL
Revenue Date	The revenue date of the transaction
Facility	The facility of the transaction
Plaza/Lane	The plaza/lane of the transaction

Exit Date/Time	The exit date/time of the transaction
Entry Date/Time	The entry date/time of the transactions
Tag #	The tag agency/serial number associated with the transaction
Pgm Stat	The tag program status
Lane Mode	The operating mode of the lane at the time of the transaction
Amount Due	The amount due for the transaction
RCS File	The number of the file (FNTX) in which this transaction was sent to the CSC
FNTX File	The number of the FNTX file in which this transaction was sent to the CSC
Recon Stat	The current CSC reconciliation code associated with the transaction

SAMPLE – ACH-0009:

Port Authority of NY & NJ - E-ZPass Plus System

Report Date 04/29/2015 | **Eligible Resubmissions Transaction Detail Report** | Report Number ACH 0009

Time 14:31:17 | Reporting Period From: 04/01/2015 To: 04/07/2015

	Exit Date/Time	Entry Date/Time	Entry Plaza	Entry Lane	Tag #	Pgm Status	Lane Mode	Amt. Due	RCS File	FNTX File	FTXN File	Recon Status
Revenue Date: 04/01/2015												
Facility : JFK Airport												
Exit Location : Lot2 (Blue Lot)												
Exit Lane : 242												
	04/01/2015 06:32:38	03/30/2015 09:48:39	JL2	264	004-05687773	S	E	$66.00	022201	104879	0	DECL
	04/01/2015 21:54:12	04/01/2015 19:46:48	JL2	264	022-05385492	S	E	$20.00	022201	104879	0	DECL
Total Amount Due For Exit Lane : 242						**Count**	**2**	**$86.00**				
Total Amount Due For Exit Location : Lot2 (Blue Lot)						**Count**	**2**	**$86.00**				
Exit Location : Garage1 (Green Lot)												
Exit Lane : 104												
	04/01/2015 17:16:45	04/01/2015 15:08:08	JG1	123	008-09725628	S	E	$20.00	022201	104879	0	DECL
	04/01/2015 21:24:38	04/01/2015 19:14:26	JG1	122	008-09023861	S	E	$20.00	022201	104879	0	DECL
	04/01/2015 22:22:47	04/01/2015 20:03:40	JG1	125	022-05832430	S	E	$20.00	022201	104879	0	DECL
Total Amount Due For Exit Lane : 104						**Count**	**3**	**$60.00**				
Exit Lane : 106												
	04/01/2015 21:03:16	04/01/2015 18:57:36	JG1	124	005-02206158	S	E	$20.00	022201	104879	0	DECL
	04/02/2015 00:35:18	04/01/2015 20:53:03	JG1	121	006-01540713	S	E	$32.00	022201	104879	0	DECL
Total Amount Due For Exit Lane : 106						**Count**	**2**	**$52.00**				
Exit Lane : 107												
	04/01/2015 15:31:27	04/01/2015 12:40:46	JG1	122	008-06516464	S	E	$24.00	022201	104879	0	DECL
	04/01/2015 16:34:20	04/01/2015 14:12:11	JG1	123	008-06415934	S	E	$20.00	022201	104879	0	DECL
Total Amount Due For Exit Lane : 107						**Count**	**2**	**$44.00**				
Total Amount Due For Exit Location : Garage1 (Green Lot)						**Count**	**7**	**$156.00**				

ACH-0008 Declined Write-Off Summary Report

Run Date: MM/DD/YYYY
Run Time: HH:MM
Run By: XXXXXXXXXXXXXXX

Port Authority of NY & NJ - E-ZPass Plus System
Declined Write-Off Summary Report

Page N of M
ACH-0008

Period: MM/DD/YYYY through MM/DD/YYYY

Revenue Date	EWR		JFK		LGA		Date Total	
	# Trans	Amount	# Trans	Amount	# Trans	Amount	# Trans	Amount
MM/DD/YYYY	###,###	$###,###.##	###,###	$###,###.##	###,###	$###,###.##	###,###	$###,###.##
.	.		.		.		.	
.	.		.		.		.	
.	.		.		.		.	
.	.		.		.		.	
.	.		.		.		.	
.	.		.		.		.	
.	.		.		.		.	
Report Totals	###,###	$#,###,###.##	###,###	$#,###,###.##	###,###	$#,###,###.##	###,###	$#,###,###.##

Report Parameters:

Period start date	The user supplied start date (based on revenue date) of the reporting period
Period end date	The user supplied end date (based on revenue date) of the reporting period

Report Usage:

This report shows a summary breakdown of the number of E-ZPass Plus transactions which were reconciled by the CSC as DECL or NOCC and are no longer eligible for resubmission via the corrections file or have been declined a second time.

Field Definitions:

Run Date	Date the report is being executed
Run Time	The time the report is being executed
Run By	The user running the report
Period:	The period covered by the report
Revenue Date	The revenue date of the summary data

EWR	The number/value of write-off E-ZPass Plus transactions for EWR for the given summary date
JFK	The number/value of write-off E-ZPass Plus transactions for JFK for the given summary date
LGA	The number/value of write-off E-ZPass Plus transactions for LGA for the given summary date
Date Total	The total number/value of write-off E-ZPass Plus transactions for the given summary date
Report Totals	Totals for the columns shown for the Period

SAMPLE – ACH-0008:

Port Authority of NY & NJ - E-ZPass Plus System

Declined Writeoff Summary Report

Report Date 04/29/2015
Time 14:44:49

Report Number ACH 0008

Reporting Period From: 01/01/2015 To: 01/31/2015

	EWR		JFK		LGA		Total	
Revenue Date	Count	Amount	Count	Amount	Count	Amount	Count	Amount
01/01/2015	6	$1,082.00	13	$797.00	1	$78.00	20	$1,957.00
01/02/2015	7	$1,001.00	7	$1,009.00	2	$270.00	16	$2,280.00
01/03/2015	6	$428.00	13	$1,174.00	3	$399.00	22	$2,001.00
01/04/2015	9	$460.00	16	$1,078.00	2	$40.00	27	$1,578.00
01/05/2015	3	$402.00	11	$2,055.00	4	$424.00	18	$2,881.00
01/06/2015	3	$142.00	16	$817.00	4	$483.00	23	$1,442.00
01/07/2015	6	$411.00	12	$386.00	0	$0.00	18	$797.00
01/08/2015	6	$629.00	8	$326.00	1	$20.00	15	$975.00
01/09/2015	2	$53.00	11	$517.00	3	$188.00	16	$758.00
01/10/2015	1	$24.00	11	$432.00	1	$162.00	13	$618.00
01/11/2015	5	$363.00	14	$965.00	4	$336.00	23	$1,664.00
01/12/2015	5	$531.00	6	$402.00	2	$147.00	13	$1,080.00
01/13/2015	3	$476.00	6	$477.00	4	$260.00	13	$1,213.00
01/14/2015	4	$245.00	5	$142.00	5	$304.00	14	$691.00
01/15/2015	4	$267.00	6	$237.00	2	$285.00	12	$789.00
01/16/2015	10	$936.00	7	$674.00	0	$0.00	17	$1,610.00
01/17/2015	4	$349.00	6	$367.00	0	$0.00	10	$716.00
01/18/2015	9	$485.00	6	$267.00	2	$141.00	17	$893.00
01/19/2015	7	$927.00	8	$551.00	3	$243.00	18	$1,721.00
01/20/2015	8	$584.00	6	$314.00	2	$824.00	16	$1,722.00
01/21/2015	8	$715.00	11	$875.00	1	$252.00	20	$1,842.00
01/22/2015	7	$504.00	5	$100.00	1	$20.00	13	$624.00
01/23/2015	9	$621.00	4	$161.00	2	$91.00	15	$873.00
01/24/2015	7	$575.00	5	$142.00	1	$24.00	13	$741.00
01/25/2015	8	$626.00	8	$673.00	6	$599.00	22	$1,898.00
01/26/2015	7	$402.00	3	$283.00	0	$0.00	10	$685.00
01/27/2015	0	$0.00	1	$165.00	0	$0.00	1	$165.00

ACH-0007 Declined Write-Off Transaction Detail Report

Run Date:	MM/DD/YYYY	Port Authority of NY & NJ - E-ZPass Plus System	Page N of M
Run Time:	HH:MM	Declined Write-Off Transaction Detail Report	ACH-0007
Run By:	XXXXXXXXXXXXXXX		

Period: MM/DD/YYYY through MM/DD/YYYY

Facility: XXX Plaza/Lane: XXXXX

Revenue Date	Facility	Exit Plaza/ Lane	Exit Date/Time	Entry Date/Time	Entry Plaza/ Lane	Tag #	Pgm Stat	Lane Mode	Amout Due	RCS File	FNTX File	Recon Stat	FTXN File	Corr Recon Stat
MM/DD/YYYY	XXX	PPPP/LLLL	MM/DD/YYYY HH:MM:SS	MM/DD/YYYY HH:MM:SS	PPPP/LLLL	###-#######	X	XXXXX	$###,###.##	#########	#########	XXXX	#########	XXXX
.		.	. . .	.										
.		.	. . .	.										
.		.	. . .	.										
.		.	. . .	.										
.		.	. . .	.										
.		.	. . .	.										

Report Parameters:

Period start date/time	The user supplied start date (based on revenue date) of the reporting period
Period end date/time	The user supplied end date (based on revenue date) of the reporting period
Facility:	The user supplied airport to be reported on or ALL for all airports
Plaza/Lane:	The user supplied airport plaza/lane to be reported on or ALL for all plazas/lanes at the selected airport

Report Usage:

This report shows details of E-ZPass Plus transactions sent to the CSC that
have been reconciled back as DECL or NOCC and are no longer eligible for resubmission
either because the time for resubmission has expired or because they were declined a second time.

Field Definitions:

Run Date	Date the report is being executed
Run Time	The time the report is being executed
Run By	The user running the report
Period:	The period covered by the report

Facility:	The facility represented in the report or ALL if all are combined
Plaza/Lane:	The plaza/lane represented in the report of ALL
Revenue Date	The revenue date of the transaction
Facility	The facility of the transaction
Plaza/Lane	The plaza/lane of the transaction
Exit Date/Time	The exit date/time of the transaction
Entry Date/Time	The entry date/time of the transactions
Tag #	The tag agency/serial number associated with the transaction
Pgm Stat	The tag program status
Lane Mode	The operating mode of the lane at the time of the transaction
Amount Due	The amount due for the transaction
RCS File	The number of the file (FNTX) in which this transaction was sent to the CSC
FNTX File	The number of the FNTX file in which this transaction was sent to the CSC
Recon Stat	The CSC reconciliation code associated with the transactions original submission to the CSC
FTXN File	The number of the FTXN file in which this transaction was sent to the CSC
Corr Recon Stat	The CSC reconciliation code associated with the transactions correction submission to the CSC

SAMPLE – ACH-0007:

Port Authority of NY & NJ - E-ZPass Plus System

Declined Writeoff Transaction Detail Report

Report Date 04/29/2015
Time 13:56:45

Reporting Period From: 01/01/2015 To: 01/31/2015

Report Number ACH 0007

	Exit Date/Time	Entry Date/Time	Entry Plaza	Entry Lane	Tag #	Pgm Status	Lane Mode	Amt. Due	RCS File	FNTX File	FTXN File	Recon Status
Revenue Date: 01/01/2015												
Facility : JFK Airport												
Exit Location : Lot2 (Blue Lot)												
Exit Lane : 245												
	01/01/2015 15:27:23	01/01/2015 03:43:36	JL2	263	008-09461045	S	E	$33.00	022111	104789	0	XDECL
	01/01/2015 20:46:30	01/01/2015 18:21:53	JL2	264	008-09854662	S	E	$20.00	022111	104789	0	XDECL
Total Amount Due For Exit Lane : 245						Count	2	$53.00				
Exit Lane : 247												
	01/01/2015 22:07:37	01/01/2015 20:05:03	JL2	267	008-10006693	S	E	$20.00	022111	104789	0	XDECL
Total Amount Due For Exit Lane : 247						Count	1	$20.00				
Exit Lane : 244												
	01/01/2015 10:48:40	01/01/2015 08:47:17	JL2	264	008-08672438	S	E	$20.00	022111	104789	0	XDECL
Total Amount Due For Exit Lane : 244						Count	1	$20.00				
Total Amount Due For Exit Location : Lot2 (Blue Lot)						Count	4	$93.00				
Exit Location : Garage1 (Green Lot)												
Exit Lane : 106												
	01/01/2015 21:37:35	01/01/2015 19:31:15	JG1	122	022-07115506	S	E	$20.00	022111	104789	0	XDECL
Total Amount Due For Exit Lane : 106						Count	1	$20.00				
Total Amount Due For Exit Location : Garage1 (Green Lot)						Count	1	$20.00				
Exit Location : Lot3 (Red Lot)												
Exit Lane : 304												
	01/01/2015 09:20:37	01/01/2015 06:04:20	JL3	323	008-08263826	S	E	$28.00	022111	104789	0	XDECL
Total Amount Due For Exit Lane : 304						Count	1	$28.00				

ACH-0006 Tag File Report

Run Date: MM/DD/YYYY
Run Time: HH:MM
Run By: XXXXXXXXXXXXXXX

Port Authority of NY & NJ - E-ZPass Plus System
Tag File Report

Page N of M
ACH-0006

Period: MM/DD/YYYY through MM/DD/YYYY

Date/Time	Tag File	Valid Tags	Other Tags	Total Tags	Sanity Status
MM/DD/YYYY HH:MM:SS	XXXXXXXXXXXXXXXXXX	###,###,###	###,###,###	###,###,###	XXXXX
.	.	.	.	.	
.	.	.	.	.	
.	.	.	.	.	
.	.	.	.	.	
.	.	.	.	.	
.	.	.	.	.	
.	.	.	.	.	

Report Parameters:

Period start date	The user supplied start date of the reporting period
Period end date	The user supplied end date of the reporting period

Report Usage:

This report shows information on the tag files processed by the ACH.

Field Definitions:

Run Date	Date the report is being executed
Run Time	The time the report is being executed
Run By	The user running the report
Period:	The period covered by the report
Date/Time	The date/time the file was processed
Tag File	The name of the tag status file
Valid Tags	The count of valid tags in the file

Other Tags	The count of tags with a status other than valid in the file
Total Tags	The total number of tags in the file
Sanity Status	Indicates whether or not the file passed the sanity check

SAMPLE – ACH-0006:

Port Authority of NY & NJ - E-ZPass Plus System

Tag File Report

Report Date 04/29/2015 Report Number ACH 0006

Time 13:41:38 Reporting Period From: 04/01/2015 To: 04/29/2015

Date/Time	Tag File	Version No	Valid Tags	Other Tags	Total Tags
04/01/2015 05:09:24	008_20150401010444.FTAG	104,656	12,548,407	0	12,557,288
04/02/2015 05:09:31	008_20150402004513.FTAG	104,657	12,536,118	0	12,545,001
04/03/2015 05:09:33	008_20150403005940.FTAG	104,658	12,539,817	0	12,548,700
04/04/2015 05:16:19	008_20150404012127.FTAG	104,659	12,540,989	0	12,549,875
04/05/2015 05:10:15	008_20150405004657.FTAG	104,660	12,539,932	0	12,548,818
04/06/2015 05:09:20	008_20150406004740.FTAG	104,661	12,535,730	0	12,544,616
04/07/2015 05:09:43	008_20150407004737.FTAG	104,662	12,535,636	0	12,544,532
04/08/2015 05:09:11	008_20150408004027.FTAG	104,663	12,535,545	0	12,544,442
04/09/2015 05:09:58	008_20150409005908.FTAG	104,664	12,539,505	0	12,548,417
04/10/2015 05:09:51	008_20150410004058.FTAG	104,665	12,544,487	0	12,553,404
04/11/2015 05:15:22	008_20150411003805.FTAG	104,666	12,554,066	0	12,562,995
04/12/2015 05:10:07	008_20150412003945.FTAG	104,667	12,560,410	0	12,569,340
04/13/2015 05:09:20	008_20150413010656.FTAG	104,668	12,556,865	0	12,565,795
04/14/2015 05:16:52	008_20150414004536.FTAG	104,669	12,557,828	0	12,566,759
04/15/2015 05:09:45	008_20150415012023.FTAG	104,670	12,572,252	0	12,581,193
04/16/2015 05:09:40	008_20150416005352.FTAG	104,671	12,573,674	0	12,582,621
04/17/2015 05:13:00	008_20150417004836.FTAG	104,672	12,580,052	0	12,588,997
04/18/2015 05:16:27	008_20150418005323.FTAG	104,673	12,582,283	0	12,591,236
04/19/2015 05:09:55	008_20150419005103.FTAG	104,674	12,582,576	0	12,591,529
04/20/2015 05:09:27	008_20150420004037.FTAG	104,675	12,581,834	0	12,590,787
04/21/2015 05:09:08	008_20150421004344.FTAG	104,676	12,584,732	0	12,593,691
04/22/2015 05:08:55	008_20150422004708.FTAG	104,677	12,590,144	0	12,599,100
04/23/2015 05:09:17	008_20150423005748.FTAG	104,678	12,590,912	0	12,599,874
04/24/2015 23:05:23	008_20150424010320.FTAG	104,679	12,597,272	0	12,606,238
04/25/2015 05:16:17	008_20150425005039.FTAG	104,680	12,599,341	0	12,608,308
04/26/2015 05:10:02	008_20150426010430.FTAG	104,681	12,598,446	0	12,607,414
04/27/2015 05:09:25	008_20150427005257.FTAG	104,682	12,594,252	0	12,603,220
04/28/2015 05:09:06	008_20150428013018.FTAG	104,683	12,595,444	0	12,604,414
04/29/2015 05:09:32	008_20150429003626.FTAG	104,684	12,597,643	0	12,606,617

ACH-0001 Employees Report

Run Date: MM/DD/YYYY
Run Time: HH:MM
Run By: XXXXXXXXXXXXXXX

Port Authority of NY & NJ - E-ZPass Plus System
Employees Report

Page N of M
ACH-0001

User ID	Title	Name	Hire Date	Term Date	Role	Login ID
#####	XXXXX	XXXXXXXXXXXXXXX	MM/DD/YYYY	MM/DD/YYYY	XXXXXXXXXX	XXXXXXXX
#####	XXXXX	XXXXXXXXXXXXXXX	MM/DD/YYYY	MM/DD/YYYY	XXXXXXXXXX	XXXXXXXX
#####	XXXXX	XXXXXXXXXXXXXXX	MM/DD/YYYY	MM/DD/YYYY	XXXXXXXXXX	XXXXXXXX
#####	XXXXX	XXXXXXXXXXXXXXX	MM/DD/YYYY	MM/DD/YYYY	XXXXXXXXXX	XXXXXXXX

Report Parameters
Report should be runnable for:

- A given User ID
- A given Facility or ALL facilities - Note that employees with access to multiple facilities must appear only when the report parameter of ALL is specified. When ALL is specified, employees with access to only a single facility should not be displayed.
- A Hire Date range
- A Termination Date range

SAMPLE – ACH-0001:

Port Authority of NY & NJ - E-ZPass Plus System

Employees Report

Report Date 04/29/2015 Report Number ACH 0001

Time 13:44:39 **Hire Date : 12/30/1950 - 12/30/2050** **Term Date : 12/30/1950 - 12/30/2050**

User ID	Title	Name	Hire Date	Term Date	Role	Login ID
Facility : ALL - All Facilities						
100001	APPL	mike kolb	10/04/2002	09/26/2032	Customer Service	KOLB
100002	SA	William Parks	04/20/1998	09/30/2032	System Administrator	WPARKS

ACH-0002 Codes Report

Run Date:	MM/DD/YYYY	Port Authority of NY & NJ - E-ZPass Plus System	Page N of M
Run Time:	HH:MM	Codes Report	ACH-0002
Run By:	XXXXXXXXXXXXXXX		

	Code ID	Descrip Short	Descrip Long
Code Type:	**XXXXXXXXXXXX**		
	#####	XXXXXXXXXXXXXX	XXXXXXXXXXXXXXXXXXXXXXXXXXX
	#####	XXXXXXXXXXXXXX	XXXXXXXXXXXXXXXXXXXXXXXXXXX
	#####	XXXXXXXXXXXXXX	XXXXXXXXXXXXXXXXXXXXXXXXXXX
	#####	XXXXXXXXXXXXXX	XXXXXXXXXXXXXXXXXXXXXXXXXXX

Report Parameters

Report should be runnable for:

- A single Code Type or ALL Code Types

SAMPLE – ACH-0002:

Port Authority of NY & NJ - E-ZPass Plus System

Report Date 04/29/2015 | **Codes Report** | Report Number ACH 0002

Time 13:45:38 | **As Of : 04/29/2015 13:45:38**

Code Id	Descrip Short	Descrip Long
Code Type : ACCESS_MODE		
1	View	View
2	Edit	Edit
Code Type : ACK_CREATE		
2	NOPD	NO OUTBOX PATH defined
3	NLPD	NO LOG PATH defined
4	UCOL	Unable to create/open LOG file
5	BINP	An Input parameter was bad - see LOG file
6	UCOA	Unable to create/open new ACK file
7	ECAF	Error closing ACK file
8	RATF	Could not RENAME the .ACK_TMP file
9	SQL ac FCLTY	Accessing TR_FACILITY table
10	SQL CONNECT	Could not connect to the Oracle data base

ACH-0003 Lanes Report

Run Date:	MM/DD/YYYY	Port Authority of NY & NJ - E-ZPass Plus System	Page N of M
Run Time:	HH:MM	Lanes Report	ACH-0003
Run By:	XXXXXXXXXXXXXXX		

		Lane	Lane Seq. No.
Facility:	**XXX - XXXXXXXXXX**		
	Location: XXX	**XXXXXXXXXXXX**	
		XXX	###
		XXX	###
		XXX	###
		XXX	###
		XXX	###
		XXX	###

SAMPLE – ACH-0003:

Port Authority of NY & NJ - E-ZPass Plus System

Report Date 04/29/2015 | **Lanes Report** | Report Number ACH 0003

Time 13:46:44 | **Facility Short Name : ALL** **Location ID : ALL** **Lane ID : ALL**

Lane	Lane Seq. No.
Facility : EWR - EWR Airport	
Location : E1E - Lot P1/P3	
401	0
402	0
ALL	0
Location : E41 - Lot P4-1	
811	0
812	0
ALL	0
Location : E42 - Lot P4-2	
813	0
814	0
815	0
ALL	0
Location : EAE - Terminal A	
501	0
502	0
503	0
ALL	0

ACH-0004 Locations Report

Run Date:	MM/DD/YYYY	Port Authority of NY & NJ - E-ZPass Plus System	Page N of M
Run Time:	HH:MM	Locations Report	ACH-0004
Run By:	XXXXXXXXXXXXXXX		

	Location Name	**Open Date**
Facility:	**XXX - XXXXXXXXXX**	
	XXX - XXXXXXXXXX	MM/DD/YYYY
	XXX - XXXXXXXXXX	MM/DD/YYYY
	XXX - XXXXXXXXXX	MM/DD/YYYY
	XXX - XXXXXXXXXX	MM/DD/YYYY

SAMPLE – ACH-0004:
See sample ACH-0003 – ACH-0003, 0004 and 0005 have been combined.

ACH-0005 Facilities Report

Run Date:	MM/DD/YYYY	Port Authority of NY & NJ - E-ZPass Plus System	Page N of M
Run Time:	HH:MM	Facilities Report	ACH-0005
Run By:	XXXXXXXXXXXXXXX		

Facility Name

Facility:	**XXX - XXXXXXXXXX**
Facility:	**XXX - XXXXXXXXXX**
Facility:	**XXX - XXXXXXXXXX**

SAMPLE – ACH-0005:
See sample ACH-0003 – ACH-0003, 0004 and 0005 have been combined.

CSC Transaction File Report – See Section 3.0
CSC Distribution File Report – See Section 4.0
CSC Reconciliation Report – See Section 5.0
CSC Correction File Report – See Section 6.0

These reports are the results of batch processing and are described in the appropriate sections above. They shall be made available to authorized users via the same tools which allow those users to generate/view the other reports in this Appendix.

Parking Access and Revenue Control System—Design, Installation & Maintenance

Attachment U
EZ-Pass® Interface File Reporting Specifications

Facility Operator to Customer Service Center

Interface File and Reporting Specifications

Prepared by:
The E-ZPass Reciprocity Committee
06/19/2014
Version FO 1.51e

© Copyright The Port Authority of New York and New Jersey 2000-2014. All rights reserved. This document contains trade secrets and confidential information reserved for the use of authorized members of the E-ZPass Group. No use or disclosure of this document or its contents is authorized without written permission of the Port Authority.

Table of Contents

1.0 INTRODUCTION 1

2.0 TRANSACTION PROCESSING 3

3.0 REPORTING REQUIREMENTS 3

4.0 GENERAL FILE REQUIREMENTS 3

5.0 FO TAG STATUS FILE 5

6.0 FO TRANSACTION FILE 7

7.0 FO DISTRIBUTION FILE 11

8.0 FO TRANSACTION RECONCILIATION FILE 12

9.0 FO CORRECTION FILE 14

10.0 FO CORRECTION RECONCILIATION FILE 16

11.0 ACKNOWLEDGEMENT FILE 18

12.0 TRANSMISSION METHODOLOGY 20

13.0 MODIFICATION HISTORY 21

A. HOST REPORTS 23

B. FACILITY OPERATOR REPORTS 25

C. ACKNOWLEDGEMENT FILE RETURN CODES C-1

1.0 Introduction

The IAG Reciprocity II document was developed to establish a framework in which E-ZPass Agencies could participate in tag use not directly related to tolls, for example parking fees. It is assumed that any contemplated non-toll activity will fall under the framework of Reciprocity II (and the subsequent Reciprocity III).

Actual implementation of non-toll processing requires the various Customer Service Centers to develop internal programs and procedures as well as support the IAG File and Report Specifications which were developed in response to Reciprocity II.

The following files constitute the IAG standard file structure and protocol with which a Host CSC can communicate with a Facility Operator. The fundamental concept is that transaction files from a Facility Operator are split, by the Host CSC, into smaller files for processing by each Agency/CSC. Each file in that group is subsequently reconciled back to the Facility Operator.

The purpose of this document is to establish file specification and protocol necessary for a Facility Operator to exchange information with their Host CSC. The file format and protocol are based on the IAG inter-CSC file specification.

The interface files defined are (inter-Agency/CSC files are shown in **bold** and are not a part of this specification):

File Name	File Extension	File Usage
FO Tag Status File	FTAG	The FO Tag Status File is created each day by the Host CSC for each Facility Operator serviced by the Host. The Tag Status File will contain only valid tags per Reciprocity II.
FO Transaction File	FNTX	The FO Transaction file is created once each day and sent to the Host CSC. This file contains all transactions previously accepted by the Facility Operator but not yet processed by the Host. Transaction Files contain original transactions only (not corrections or re-submittals).
FO Distribution File	FNDX	For every FO Transaction File and FO Correction File received, the Host CSC shall return an FO Distribution File back to the Facility Operator summarizing the transactions in the FO Transaction/Correction File. The file header contains the file number from the corresponding FO Transaction/Correction File. There are *n* records, one record for each Home Agency/CSC represented in the FO Transaction/Correction File. The Distribution File provides the Facility Operator with assurance that the transactions in the corresponding Transaction/Correction File have been bundled into the appropriate **INTX** file and sent to that Agency/CSC (including the Host for posting).
FO Transaction Reconciliation File	FNRX	The Host CSC will generate *n* FO Transaction Reconciliation Files for each FO Transaction File, one file for each Home Agency/CSC represented in the FO Transaction File (including the Host). These files correspond one for one to the **INRX** reconciliation files received from each Home Agency/CSC in response to an **INTX** file. The file header contains the corresponding **INTX** file number and there is one detailed record for each transaction reconciled. Per IAG rules, an **INRX** file will not be generated until all transactions in the corresponding **INTX** file have been fully processed. The FO Distribution File provides the link to the original FO Transaction File.

File Name	File Extension	File Usage
FO Correction File	FTXN	The Facility Operator uses the FO Correction File to resubmit rejected, declined or incorrect transactions*. Original transactions may be resubmitted only once and only if the most recent FO Tag Status file indicates that the corresponding tag is valid. The transactions included in a correction file may be from any Home Agency and from any time (within the processing time limits). * Note: While the FO Correction File is used to make adjustments initiated by the Facility Operator, there is no corresponding file to make adjustments initiated by the Host (i.e. reversals and disputes). These adjustments are made at the CSC and the information is related to the Facility Operator via the Host Reports.
FO Correction Reconciliation File	FRXN	The Host CSC will generate *n* FO Correction Reconciliation Files for each FO Correction File, one file for each Home Agency/CSC represented in the FO Correction File (including the Host). These files correspond one for one to the **IRXN** reconciliation files received from each Home Agency/CSC in response to an **ITXN** file. The file header contains the corresponding **ITXN** file number and there is one detailed record for each transaction reconciled. Per IAG rules, an **IRXN** file will not be generated until all transactions in the corresponding **ITXN** file have been fully processed. The FO Distribution File provides the link to the original FO Correction File.
Acknowledgement File	ACK	The Acknowledgment File shall be created, by the entity receiving a file, to inform the entity which sent the original file that the file transmitted was received in its entirety. An Acknowledgement File shall be sent for each of the above referenced files.

2.0 Transaction Processing

1. The Host CSC shall reject original and corrected transactions according to the IAG Specification, including transactions older than 60 days.

2. Non-toll transactions <$20 will be posted directly to a valid account replenished by a credit card. A transaction that is attempted to be posted to an account that is currently replenished by CASH or CHECK will be rejected as NOCC.

3. A non-toll transaction ≥ $20 will create a separate re-bill request to the credit card processor for the exact amount of the transaction. If the payment is approved by the credit card processor then the payment and the transaction should both be posted to the account. If payment is not approved, then this should be noted on the account (with some means of identifying the associated non-toll transaction), and the transaction rejected as DECL in the INRX (and FNRX) file.

3.0 Reporting Requirements

The following reports are defined for the Host and the Facility Operator. Report formats are in Appendix A & B.

Host - Two Reports are defined for the Host

The Host Agency receives IAG non-toll reports from each Home Agency. These reports indicate the amount that a Home Agency owes to a Host Agency/Facility Operator for a particular settlement period. The reports are based on data in reconciliation (INRX and IRXN) files.

For each settlement period, the Host will compile a "Facility Operator Period Transaction Summary Report" (FH-1) of transactions based on Non-Toll Reconciliation (INRX) files acknowledged in the settlement period and a “Facility Operator Period Correction Summary Report” (FH-2)_of transactions based on Non-Toll Correction Reconciliation (IRXN) files acknowledged in the settlement period. Fees and final settlement reports are specific to the particular Host and Facility Operator. Due to the one for one relationship of INRX/IRXN and FNRX/FRXN files, the existing IAG 1.51N reports can serve as supporting documents to reports FH-1 and FH-2. The Host Agency may choose to modify the supporting reports to remove (or add) information.

Facility Operator - The Facility Operator will generate four reports.

The first two reports, FO-1 and FO-2 are nearly identical in format to FH-1 and FH-2 above. Both reports use the FILE_DATE and FILE_TIME of the corresponding FNRX/FRXN files, to determine those files in the settlement period. This will ensure that they will match the FH-1 and FH-2 reports generated by the Host which uses the acknowledgement date of the corresponding INRX/IRXN files. Note that the definition of the FILE_DATE and FILE_TIME in the FNRX/FRXN file is NOT the same as the definition of those fields in the INRX/IRXN file.

The third report, FO-3, is nearly identical in format to IAG-2N. FO-3 provides supporting details for one row of the FO-1 report. The Facility Operator generates one FO-3 report for each row in the FO-1 report. Again, the date used to generate FO-3 is within the FNRX file while IAG-2N uses an acknowledge date.

The fourth report, FO-4, is nearly identical in format to IAG-3N. FO-4 provides supporting details for one row of the FO-2 report. The Facility Operator generates one FO-4 report for each row in the FO-2 report. Again, the date used to generate FO-4 is within the FRXN file while IAG-3N uses an acknowledge date.

4.0 General File Requirements

1. All files (except for the Acknowledgement File) shall be compressed (ZIPed) using a standard Lempel-Zif compression algorithm which should yield a compression rate of at least 75% (meaning a file will be reduced so that it is only 25% of its original size).

2. When compressed, file names shall be converted from {FILE_NAME}.{FILE_TYPE} to {FILE_NAME}_{FILE_TYPE}.ZIP and all files names shall be created using uppercase characters only. Therefore, when file “008_19971201001015.FTAG” is compressed, the compressed file shall be named “008_19971201001015_FTAG.ZIP”.

5.0 FO Tag Status File

5.1 File Type:

Variable length, LF delimited

5.2 File Name:

{HOST_AGENCY_ID}_YYYYMMDDHHMMSS.FTAG

Example: 008_20011201001015.FTAG
Tag status file created by NY CSC on 00:10:15 on 12/01/2001

5.3 File Use:

The FO Tag Status File shall be created by the Host Agency/CSC to inform the Facility Operator as to the valid tags for that Facility. This file contains tags from the entire E-ZPass region. An FO Tag Status File is created each day for each Facility Operator serviced by the Host. The file will contain only valid tags per Reciprocity II. The file contains a provision to inform the Facility Operator as to certain discounts or non-revenue status associated with each tag.

5.4 File Layout:

FO Tag Status File – Header Structure		
Field Name	**Type/Size**	**Description/Valid Values**
FILE_TYPE	CHAR(4)	FTAG
HOST_AGENCY_ID	CHAR(3)	Standard agency ID code of the Host Agency/CSC (See IAG inter-CSC file spec.)
FILE_DATE	CHAR(8)	Date file created. Format: YYYYMMDD
FILE_TIME	CHAR(6)	Time file created: Format: HHMMSS
RECORD_COUNT	CHAR(8)	Count of all tags in file. Does not include header record. Values: 00000000 – 99999999
COUNT_STAT1	CHAR(8)	Count of all tags with status code 1. Values: 00000000 – 99999999
COUNT_STAT2	CHAR(8)	Not Currently Used
COUNT_STAT3	CHAR(8)	Not Currently Used
COUNT_STAT4	CHAR(8)	Not Currently Used
DELIMITER	CHAR(1)	LF
Header Total	**62**	

FO Tag Status File - Detail Structure		
Field Name	**Type/Size**	**Description/Valid Values**
TAG_AGENCY_ID	CHAR(3)	Tag agency ID. Values: 000 – 127
TAG_SERIAL_NUMBER	CHAR(8)	Tag serial number. Values: 00000001 – 16777216
TAG_STATUS	CHAR(1)	1 – Valid
TAG_ACCT_INFO	CHAR(6)	A string of 24 bits (3 characters) converted to Hex-ASCII format (6 characters). This field is not defined by the IAG and may be defined by the Host/Facility operator.
DELIMITER	CHAR(1)	LF
Record Total	**19**	

5.5 Processing Requirements:

1. The transmission of the file to the Facility Operator as stipulated in the Transmission Methodology section.

2. In the event that an invalid header record is encountered (e.g., character data in a numeric field, etc.), the Facility Operator should reject the file and notify the Host Agency/CSC via the Acknowledgement File.

3. In the event that a invalid detail record is encountered (e.g., inappropriate TAG_STATUS, etc.), the Facility Operator should skip that record and notify the Host Agency/CSC via the Acknowledgement File.

4. The Host Agency/CSC shall perform appropriate sanity checks on the Tag Status File prior to its transmission to the Facility Operator. Such sanity checks should include testing for unusual growth in the number of tags from previous version

5. The Facility Operator must be aware that the FO Tag Status File contains only valid tags. Therefore, each new file must replace the previous file. Any tag that is not in the file is to be considered invalid.

6. The Host CSC shall incorporate into the FO Tag Status File all tags received in the Inter-CSC Tag Status File (ITAG) that have a TAG_STATUS value of 1 (valid) or 2 (low balance) and that have Bit 1 or Bit 24 of the TAG_ACCOUNT_INFO field set to a value of 1. Any tag with a TAG_STATUS value of 2 shall have that value converted to 1 for the FO Tag Status File.

6.0 FO Transaction File

6.1 File Type:

Variable length, LF delimited

6.2 File Name:

{FO _ID}_{HOST_AGENCY_ID}_YYYYMMDDHHMMSS.FNTX
Example: 128_004_20011201001015.FNTX
Albany transactions to NYSTA create on 00:10:15 on 12/01/2001

6.3 File Use:

The FO Transaction file is created once each day and sent to the Host CSC. This file contains all transactions previously accepted by the Facility Operator but not yet processed by the Host. Transaction Files contain original transactions only (not corrections or re-submittals).

6.4 File Layout:

FO Transaction File – Header Structure		
Field Name	**Type/Size**	**Description/Valid Values**
FILE_TYPE	CHAR(4)	FNTX
FO_ID	CHAR(3)	Standard ID code of the Facility Operator (See IAG Inter-CSC File Spec)
HOST_AGENCY_ID	CHAR(3)	Standard agency ID code of the Host Agency (See IAG Inter-CSC file spec)
FILE_DATE	CHAR(8)	Date file created. Format: YYYYMMDD
FILE_TIME	CHAR(6)	Time file created. Format: HHMMSS
RECORD_COUNT	CHAR(8)	Count of transactions in the file. Does not include header record. Values: 00000000 – 99999999
FNTX_FILE_NUM	CHAR(6)	A unique sequential number used to identify the FO Transaction File to the Host Agency. Values 000001 – 999999.
DELIMITER	CHAR(1)	LF
Header Total	**39**	

FO Transaction File – Detail Structure		
Field Name	**Type/Size**	**Description/Valid Values**
ETC_TRX_SERIAL_NUM	CHAR(12)	The unique key of a transaction assigned by the Facility Operator. Values: 000000000000 – 999999999999
ETC_REVENUE_DATE	CHAR(8)	The revenue date of the transaction as determined by the Facility Operator. Format: YYYYMMDD
ETC_FAC_AGENCY	CHAR(3)	A code indicating the **facility operator** at which the transaction occurred. See IAG Inter-CSC file spec
ETC_TRX_TYPE	CHAR(1)	This field is used to denote the type of transaction. Values: P - Parking Transaction
ETC_ENTRY_DATE	CHAR(8)	The date the vehicle entered the facility. Format: YYYYMMDD If not provided must be ********.
ETC_ENTRY_TIME	CHAR(6)	The time the vehicle entered the facility. Format: HHMMSS If not provided must be ******.
ETC_ENTRY_PLAZA	CHAR(3)	The ETC_FAC_AGENCY plaza code of the plaza at which the vehicle entered the facility. If not provided must be ***. This contents of this field are left justified and padded with trailing blanks as needed. Refer to IAG Inter-CSC file spec for the list of valid values for this field.

FO Transaction File – Detail Structure		
Field Name	**Type/Size**	**Description/Valid Values**
ETC_ENTRY_LANE	CHAR(3)	The ETC_FAC_AGENCY lane code of the lane at which the vehicle entered the facility. This contents of this field are left justified and padded with trailing blanks as needed. If not provided must be ***.
ETC_TAG_AGENCY	CHAR(3)	Standard agency ID read from the tag. Values: 000 – 127
ETC_TAG_SERIAL_NUMBER	CHAR(8)	Tag serial number read from the tag. Values: 00000001 – 16777215
ETC_READ_PERFORMANCE	CHAR(2)	The total number of times the tag was read while in the capture zone. Obtained from the AVI reader. Values: 00 – 99 ** if data is unavailable This would be from the exit transaction.
ETC_WRITE_PERF	CHAR(2)	The total number of times the tag was written to while in the capture zone. Obtained from the AVI reader. Values: 00 – 99 ** if data is unavailable This would be from the exit transaction.
ETC_TAG_PGM_STATUS	CHAR(1)	The result of the AVI tag program cycle. Obtained from the AVI reader. Values: S – Success U – Unverified F – Failed * if data is unavailable This would be from the exit transaction. This field along when used in conjunction with ETC_READ_PERFORMANCE and ETC_WRITE_PERF would allow the Host Agency to gauge tag performance over time.
ETC_LANE_MODE	CHAR(1)	The mode the lane was operating in at the time of the transaction. Values: E – ETC Only (Dedicated) A – ETC/ACM M – Manned/ETC This would be from the exit transaction.
ETC_VALIDATION_STATUS	CHAR(1)	The tag status from the tag status file at the time of the transaction. Values: 1 – Good * - Used if the lane system does not report this value to its CSC. This would be from the exit transaction.
ETC_LIC_STATE	CHAR(2)	Unused. Must contain **.
ETC_LIC_NUMBER	CHAR(10)	Unused. Must contain **********.
ETC_CLASS_CHARGED	CHAR(3)	Unused. Must contain ***.
ETC_ACTUAL_AXLES	CHAR(2)	The number of axles associated with the vehicle. Values: 00 – 99 If not available, should default to the number of axles encoded on the tag.
ETC_EXIT_SPEED	CHAR(3)	The speed in MPH of the vehicle as it exited the facility. If the Facility Operator cannot/does not measure speed, 000 should be used. Values: 000 – 999 This field would allow the Home Agency to gauge customer speed activity over time. It also can be used to offset low counts in the ETC_READ_PERFORMANCE and ETC_WRITE_PERF fields since vehicles traveling at higher speeds typically have lower performance figures.

FO Transaction File – Detail Structure		
Field Name	**Type/Size**	**Description/Valid Values**
ETC_OVER_SPEED	CHAR(1)	An indicator of whether or not the speed reported in ETC_EXIT_SPEED was over the allowable threshold for that plaza/lane. Values: Y – Speed is over threshold N – Speed is not over threshold
ETC_EXIT_DATE	CHAR(8)	The date the vehicle exited the facility. Format: YYYYMMDD
ETC_EXIT_TIME	CHAR(6)	The time the vehicle exited the facility. Format: HHMMSS
ETC_EXIT_PLAZA	CHAR(3)	The ETC_FAC_AGENCY plaza code of the plaza at which the vehicle exited the facility. This contents of this field are left justified and padded with trailing blanks as needed. Refer to IAG Inter-CSC file spec for the list of valid values for this field.
ETC_EXIT_LANE	CHAR(3)	The ETC_FAC_AGENCY lane code of the lane at which the vehicle exited the facility. This contents of this field are left justified and padded with trailing blanks as needed.
ETC_DEBIT_CREDIT	CHAR(1)	An indicator as to whether the amount reflected in ETC_AMOUNT_DUE is to be debited from the customer account or credited to the customer account. Values: Plus (+) – Debit from customer account Space ( ) – Debit from customer account Minus (-) – Credit to customer account
ETC_AMOUNT_DUE	CHAR(7)	The amount due as calculated by the Facility Operator. Values: 0000000 ($00000.00) – 9999999 ($99999.99)
DELIMITER	CHAR(1)	LF
Record Total	**112**	

6.5 Processing Requirements:

1. The FO Transaction File is separated by the Host CSC into individual INTX files and sent to the appropriate Home CSC for processing. As such, the Host CSC should expect a corresponding INRX file from the Home CSC when all of the transactions in the INTX are processed. As they are received, the INRX files are translated into FNRX files and sent to the Facility Operator. The Host CSC must produce an FNRX file for ALL Home CSCs including those transactions posted to its own accounts.

2. It shall be the responsibility of the Facility Operator to ensure that the FO Transaction File does not contain two (or more) transactions for the same ETC_TAG_AGENCY/ ETC_TAG_SERIAL_NUMBER combination in the same ETC_EXIT_PLAZA within a five (5) minute period.

3. A credit transaction must have it own unique ETC_TRX_SERIAL_NUM but may share the same agency, plaza, lane and date/time information so that it may be accurately reflected on the customer account and statement. This duplication of agency, plaza, lane and date/time information should not be considered a duplicate as discussed in requirement #1. This field should NOT be used in lieu of the Correction File. Its primary use is to generate credit transactions in the same file as the original debit transaction.

4. Transactions originating at parking facilities will be sent with a value of ‘P’ in the ETC_TRX_TYPE field. Entry information (fields ETC_ENTRY_DATE, ETC_ENTRY_TIME, ETC_ENTRY_PLAZA and ETC_ENTRY_LANE) is optional for parking transactions in that it may be provided or may be filled with asterisks (*). Exit information (ETC_EXIT_DATE, ETC_EXIT_TIME, ETC_EXIT_PLAZA and ETC_EXIT_LANE) must always be provided.

5. The combination of FO_ID and FNTX_FILE_NUM forms a unique sequential key which will be used by the receiving agency (the Home Agency) to verify that each FO Transaction File was received without any gaps.

   If the FNTX_FILE_NUM of the current FO Transaction File does not equal the prior FNTX_FILE_NUM received from that Facility Operator plus one (1), the Acknowledgement File shall contain a

RETURN_CODE of ‘04’ to signify that a gap in sequence numbers was found. However, the current FO Transaction File should still be processed.

If the FNTX_FILE_NUM of the current FO Transaction File is equal to the FNTX_FILE_NUM of a previous FO Transaction File, the Acknowledgement File shall contain the appropriate RETURN_CODE and the current FO Transaction File should not be processed.

6. Transactions shall be routed to a Home Agency/CSC based on the data contained in CSC/Agency Cross Reference found in the IAG Inter-CSC file spec.

7. Each FO Transaction File shall only contain transactions from a single Facility Operator (based on the ETC_FAC_AGENCY code in the detail transactions).

7.0 FO Distribution File

7.1 File Type:

Variable length, LF delimited

7.2 File Name:

{HOST_AGENCY_ID}_{FO_ID}_YYYYMMDDHHMMSS.FNDX

Example: 004_128_20011201041015.FNDX
NYSTA distribution data to Albany created on 04:10:15 on 12/01/2001

7.3 File Use:

For every FO Transaction or FO Correction File received, the Host CSC shall return an FO Distribution File back to the Facility Operator summarizing the transactions in the FO Transaction/Correction File. The file header contains the file number from the corresponding FO Transaction/Correction File as well as an indicator as to the file type (Transaction vs. Correction). There are *n* records, one record for each Home Agency/CSC represented in the FO Transaction/Correction File. The Distribution File provides the Facility Operator with assurance that the transactions in the corresponding Transaction/Correction File have been bundled into the appropriate **INTX/ITXN** file and sent to that Agency/CSC (including the Host) for posting.

7.4 File Layout:

FO Distribution File – Header Structure		
Field Name	**Type/Size**	**Description/Valid Values**
FILE_TYPE	CHAR(4)	FNDX
HOST_AGENCY_ID	CHAR(3)	Standard agency ID code of the Host Agency (See IAG Inter-CSC file spec)
FO_ID	CHAR(3)	Standard agency ID code of the Facility Operator (See IAG Inter-CSC file spec)
FILE_DATE	CHAR(8)	Date file created. Format: YYYYMMDD
FILE_TIME	CHAR(6)	Time file created. Format: HHMMSS
RECORD_COUNT	CHAR(8)	Count of transactions in the file. Does not include header record. Values: 00000000 – 99999999
DIST_TYPE	CHAR(4)	Indicates the type of file to which this distribution file applies. Values: FNTX - Transaction File Distribution FTNX - Correction File Distribution
TX_FILE_NUM	CHAR(6)	The file number of the FNTX/FTXN file to which this FNDX file is associated. Values: 000001 – 999999.
DELIMITER	CHAR(1)	LF
Header Total	**43**	

FO Distribution File – Detail Structure		
Field Name	**Type/Size**	**Description/Valid Values**
DIS_HOME_AGENCY_ID	CHAR(3)	Standard agency ID code of the Home Agency/CSC to which a set of transactions were sent in an INTX file.
DIS_TX_NUM	CHAR(6)	The INTX/ITXN file number in which the transactions were sent.
DIS_NUM_TRANS	CHAR(8)	The number of transactions sent in the associated INTX/ITXN file.
DIS_AMOUNT	CHAR(12)	The total dollar value for the transactions sent in the associated INTX /ITXNfile. Values: 000000000000 ($0000000000.00) – 999999999999 ($9,999,999,999.99)
DELIMITER	CHAR(1)	LF
Record Total	**30**	

7.5 Processing Requirements:

1. The Distribution file provides the one-to-many link between FO Transaction/Correction Files (FNTX/FTXN) and FO Transaction/Correction Reconciliation files (FNRX/FRXN).

8.0 FO Transaction Reconciliation File

8.1 File Type:

Variable length, LF delimited

8.2 File Name:

{HOME_AGENCY_ID}_{FO_ID}_YYYYMMDDHHMMSS.FNRX

Example: 022_128_20011201041015.FNRX
Consortium reconciliation data to Albany. The date and time represents when the corresponding INRX file was acknowledged by the Host (NYSTA) to the Home (Regional Consortium) (on 04:10:15 on 12/01/2001).

8.3 File Use:

The Host CSC will generate *n* FO Transaction Reconciliation Files for each FO Transaction File, one file for each Home Agency/CSC represented in the FO Transaction File (including the Host). These files correspond one for one to the **INRX** reconciliation files received from each Home Agency/CSC in response to an **INTX** file. The file header contains the corresponding **INTX** file number and there is one detailed record for each transaction reconciled. Per IAG rules, an **INRX** file will not be generated until all transactions in the corresponding **INTX** file have been fully processed. The FO Distribution File provides the link to the original FO Transaction File.

8.4 File Layout:

FO Transaction Reconciliation File – Header Structure		
Field Name	**Type/Size**	**Description/Valid Values**
FILE_TYPE	CHAR(4)	FNRX
HOME_AGENCY_ID	CHAR(3)	Standard agency ID code of the Home Agency/CSC (See IAG Inter-CSC file spec)
FO_ID	CHAR(3)	Standard agency ID code of the Facility Operator (See IAG Inter-CSC file spec.
FILE_DATE	CHAR(8)	Date the corresponding INRX file was acknowledged. Format: YYYYMMDD
FILE_TIME	CHAR(6)	Time the corresponding INRX file was acknowledged. Format: HHMMSS
RECORD_COUNT	CHAR(8)	Count of transactions in the file. Does not include header record. Values: 00000000 – 99999999
INTX_FILE_NUM	CHAR(6)	The file number of the INTX file to which this FNRX file is associated. Values: 000001 – 999999.
DELIMITER	CHAR(1)	LF
Header Total	**39**	

FO Transaction Reconciliation File – Detail Structure		
Field Name	**Type/Size**	**Description/Valid Values**
ETC_TRX_SERIAL_NUM	CHAR(12)	The unique key of the transaction assigned by the Facility Operator. Values: 000000000000 – 999999999999
ETC_POST_STATUS	CHAR(4)	The result of the Home Agency's/CSC's attempt to post the transaction. Values: PSNT - Non-Toll transaction posted successfully. DECL - Credit card declined. Only used for transactions passed directly through to the credit card. NOCC - Rejected, attempt was made to post the transaction to an account that is no longer a credit card account. RJIN - Rejected, the account had insufficient funds to post the transaction. Used for non-credit card based accounts. RJCX - Rejected, the transaction is an attempt to correct a transaction which has already been corrected.

FO Transaction Reconciliation File – Detail Structure		
Field Name	**Type/Size**	**Description/Valid Values**
		RINV - Rejected, the transaction contains invalid data (e.g., invalid agency as defined in IAG Inter-CSC file spec Appendix A, invalid plaza as defined in Appendix B, invalid class as defined in Appendix C, etc.) TAGB – Rejected, tag in bad status (e.g., lost, stolen, etc.) where transaction date/time (ETC_EXIT_DATE/ ETC_EXIT_TIME) is greater than date/time of acknowledgement from that Away Agency/CSC of receipt of full Tag Status File which indicated that the tag was in a Lost/Stolen status. ACCC - Rejected, account was in a closed status at the time the post was attempted. This code is used regardless of the status of the account at the time of the transaction. OLD3 - Rejected, old transaction – The difference between the date of the transaction and the date the transaction was received by the Home Agency/CSC exceeded that specified in the Non-Toll Reciprocity Agreement. RJDP - Rejected, duplicate transaction. Usually associated with a skip read or cross lane read where a tagged transaction and license plate transaction exist for the same customer at the same plaza within five (5) minutes. The license plate transaction is rejected as the duplicate.
ETC_POST_PLAN	CHAR(5)	The Facility Operator discount plan used when the transaction was posted. This is only applicable when the Home Agency/CSC offers the Facility Operator discount plans to its customers. Values: 00002 - PANYNJ Non-Revenue If no discount plan is used, this field shall be blank.
ETC_DEBIT_CREDIT	CHAR(1)	An indicator as to whether the amount reflected in ETC_OWED_AMOUNT is to be applied to the amount owed to the Facility Operator or removed from that amount. Values: Plus (+) – Apply to amount owed Space ( ) – Apply to amount owed Minus (-) – Remove from amount owed
ETC_OWED_AMOUNT	CHAR(7)	The amount owed to the Facility Operator. For rejected transactions, this would be 0000000. Values: 0000000 ($00000.00) – 9999999 ($99999.99)
DELIMITER	CHAR(1)	LF
Record Total	**30**	

8.5 Processing Requirements:

1. The Host CSC is to send FNRX files to the Facility Operator as INRX files are received from other CSCs or produced internally when transactions are posted to Host accounts. (See FO transaction File processing requirement #1).

2. An ETC_POST_STATUS of RJIN should normally not be used since the definition of E-ZPass Plus is that the accounts be credit card backed. Therefore, if an account no longer has a credit card associated with it, the ETC_POST_STATUS of NOCC should be used. However, the code of RJIN was added to allow for the case whereby a Home Agency/CSC wanted to utilize a business rule that allowed transactions valued at < $20.00 to post against an account even if the credit card was no longer associated with said account. In such cases, if the account had insufficient funds to allow the non-toll transaction to post, an ETC_POST_STATUS of RJIN would be returned.

3. Transactions with an ETC_POST_STATUS of DECL or NOCC should be placed in a holding queue by the Facility Operator for potential resubmission via the FO Correction File. See Section 9.5 for additional details.

9.0 FO Correction File

9.1 File Type:

Variable length, LF delimited

9.2 File Name:

{FO_ID}_{HOST_AGENCY_ID}_YYYYMMDDHHMMSS.FTXN

Example: 128_004_20011201001015.FTXN
Albany transactions to NYSTA create on 00:10:15 on 12/01/2001

9.3 File Use:

The Facility Operator uses the FO Correction File to resubmit rejected, declined or incorrect transactions*. Original transactions may be resubmitted only once and only if the most recent FO Tag Status file indicates that the corresponding tag is valid. The transactions included in a correction file may be from any Home Agency and from any time (within the processing time limits). FO Correction Files may not be sent more frequently than once per week.

* Note: While the FO Correction File is used to make adjustments initiated by the Facility Operator, there is no corresponding file to make adjustments initiated by the Host (i.e. reversals and disputes). These adjustments are made at the CSC and the information is related to the Facility Operator via the Host Reports.

9.4 File Layout:

FO Correction File – Header Structure		
Field Name	**Type/Size**	**Description/Valid Values**
FILE_TYPE	CHAR(4)	FTXN
FO_ID	CHAR(3)	Standard agency ID code of the Facility Operator (See IAG Inter-CSC file spec.)
HOST_AGENCY_ID	CHAR(3)	Standard agency ID code of the Host Agency (See IAG Inter-CSC file spec)
FILE_DATE	CHAR(8)	Date file created. Format: YYYYMMDD
FILE_TIME	CHAR(6)	Time file created. Format: HHMMSS
RECORD_COUNT	CHAR(8)	Count of transactions in the file. Does not include header record. Values: 00000000 – 99999999
FTXN_FILE_NUM	CHAR(6)	A unique sequential number used to identify the FO Correction File to the Host Agency. Values 000001 – 999999.
DELIMITER	CHAR(1)	LF
Header Total	**39**	

FO Correction File – Detail Structure		
Field Name	**Type/Size**	**Description/Valid Values**
CORR_REASON	CHAR(2)	A code denoting the reason for the correction. Values: 03 – Ignore tagged transaction 04 – Corrected plaza/lane information 05 – Corrected amount 06 - Repost attempt requested
All other fields from the FO Transaction File	CHAR(112)	All fields from the original transaction (refer to FO Transaction File structure for details) will be retransmitted with the appropriate fields corrected to their required values.
Record Total	**114**	

9.5 Processing Requirements:

1. The combination of FO_ID and FTXN_FILE_NUM forms a unique sequential key which will be used by the receiving agency (the Host Agency) to verify that each FO Correction File was received without any gaps.

   If the FTXN_FILE_NUM of the current Correction File does not equal the prior FTXN_FILE_NUM received from that FO_ID plus one (1), the Acknowledgement File shall contain a RETURN_CODE of '04' to signify

that a gap in sequence numbers was found. However, the current FO Correction File should still be processed.

If the FTXN_FILE_NUM of the current FO Correction File is equal to the FTXN_FILE_NUM of a previous FO Correction File, the Acknowledgement File shall contain the appropriate RETURN_CODE and the current FO Correction File should not be processed.

2. Transactions can only be sent in a Correction File once. Subsequent corrections to the same transaction, if required, must be handled manually.

3. The FO Correction File is separated by the Host CSC into individual ITXN files and sent to the appropriate Home CSC for processing. As such, the Host CSC should expect a corresponding IRXN file from the Home CSC when all of the transactions in the ITXN are processed. As they are received, the IRXN files are translated into FRXN files and sent to the Facility Operator. The Host CSC must produce an FRXN file for ALL Home CSCs including those corrections posted to its own accounts.

4. This file can only contain transactions that have been previously submitted via an FO Transaction File. If the Host CSC detects transactions in this file for which a transaction was not previously received in an FO Transaction File, the Host CSC shall reject the entire FO Correction File with a RETURN_CODE of ‘02’ in the corresponding Acknowledgement File.

5. As indicated in Section 8.5, the Facility Operator should maintain a holding queue of transactions reconciled with an ETC_POST_STATUS of DECL or NOCC. On a daily basis, the Facility Operator system should check the incoming FO Tag Status File to see if tags associated with transactions in the holding queue are present in the FO Tag Status File. If such a match is found, it means that the account associated with the tag is again valid for non-tolls and the Facility Operator may resubmit the associated transaction to the Host CSC via the FO Correction File with a CORR_REASON value of ‘06’.

   Note that transactions can only remain in the holding queue until the transaction date has exceeded the timeframe allowed for resubmissions as defined in the Non-Toll Reciprocity Agreement. Once that timeframe has been exceeded, such transactions cannot be resubmitted and must be removed from the holding queue. The Facility Operator may manually request from the Home CSC the name and address associated with the given tag so that the Facility Operator may pursue payment of the required non-toll fee.

10.0 FO Correction Reconciliation File

10.1 File Type:

Variable length, LF delimited

10.2 File Name:

{HOME_AGENCY_ID}_{FO_AGENCY_ID}_YYYYMMDDHHMMSS.FRXN

Example: 022_128_20011201041015.FRXN
Regional Consortium reconciliation to Albany . The date and time represents when the corresponding IRXN file was acknowledged by the Host (NYSTA) to the Home (Regional Consortium) (on 04:10:15 on 12/01/2001).

10.3 File Use:

The Host CSC will generate *n* FO Correction Reconciliation Files for each FO Correction File, one file for each Home Agency/CSC represented in the FO Correction File (including the Host). These files correspond one for one to the **IRXN** reconciliation files received from each Home Agency/CSC in response to an **ITXN** file. The file header contains the corresponding **ITXN** file number and there is one detailed record for each transaction reconciled. Per IAG rules, an **IRXN** file will not be generated until all transactions in the corresponding **ITXN** file have been fully processed. The FO Distribution File provides the link to the original FO Correction File.

10.4 File Layout:

FO Correction Reconciliation File – Header Structure		
Field Name	**Type/Size**	**Description/Valid Values**
FILE_TYPE	CHAR(4)	FRXN
HOME_AGENCY_ID	CHAR(3)	Standard agency ID code of the Home Agency (See IAG Inter-CSC file spec.)
FO_ID	CHAR(3)	Standard agency ID code of the Facility Operator (See IAG Inter-CSC file spec.)
FILE_DATE	CHAR(8)	Date the corresponding IRXN file was acknowledged. Format: YYYYMMDD
FILE_TIME	CHAR(6)	Time the corresponding IRXN file was acknowledged. Format: HHMMSS
RECORD_COUNT	CHAR(8)	Count of transactions in the file. Does not include header record. Values: 00000000 – 99999999
ITXN_FILE_NUM	CHAR(6)	The file number of the ITXN file to which this FRXN file is associated. Values: 000001 – 999999.
DELIMITER	CHAR(1)	LF
Header Total	**39**	

FO Correction Reconciliation File – Detail Structure		
Field Name	**Type/Size**	**Description/Valid Values**
Same fields as the FO Transaction Reconciliation File	CHAR(30)	Same as the FO Transaction Reconciliation File.

10.5 Processing Requirements:

1. The Host CSC is to send FRXN files to the Facility Operator as IRXN files are received from other CSCs or produced internally when transactions are posted to Host accounts. (See FO Correction File processing requirement #3).

2. An ETC_POST_STATUS of RJIN should normally not be used since the definition of E-ZPass Plus is that the accounts be credit card backed. Therefore, if an account no longer has a credit card associated with it, the ETC_POST_STATUS of NOCC should be used. However, the code of RJIN was added to allow for the case whereby a Home Agency/CSC wanted to utilize a business rule that allowed transactions valued

at < $20.00 to post against an account even if the credit card was no longer associated with said account. In such cases, if the account had insufficient funds to allow the non-toll transaction to post, an ETC_POST_STATUS of RJIN would be returned.

11.0 Acknowledgement File

11.1 File Type:

Fixed length, LF delimited

11.2 File Name:

{FROM_ID}_{FILE_NAME}_{FILE_TYPE}.ACK

Example: 128_004_20011201041015_FTAG.ACK
Acknowledgement file from Albany in response to the NYSTA tag status file created on 04:10:15 on 12/01/2001

11.3 File Use:

The Acknowledgment File shall be created, by the entity receiving a file, to inform the entity which sent the original file that the file transmitted was received in its entirety. An Acknowledgement File shall be sent for each of the above referenced files.

11.4 File Layout:

Acknowledgment File - Detail Structure		
Field Name	**Type/Size**	**Description/Valid Values**
FILE_TYPE	CHAR(4)	ACK
FROM_ID	CHAR(3)	Standard agency ID code of the entity which received the file referenced in ORIG_FILE_NAME_TYPE.
TO_ID	CHAR(3)	Standard agency ID code of the entity which sent the file referenced in ORIG_FILE_NAME_TYPE.
ORIG_FILE_NAME_TYPE	CHAR(50)	The name and type of the file being acknowledged as received from the To Agency. Format: FILE_NAME.FILE_TYPE where FILE_NAME is the name of the file being acknowledged and FILE_TYPE is the type of the file being acknowledged.
FILE_DATE	CHAR(8)	Date ACK file created. Format: YYYYMMDD This is to be used by the To Agency/CSC as the acknowledgement date.
FILE_TIME	CHAR(6)	Time ACK file created. Format: HHMMSS This is to be used by the To Agency/CSC as the acknowledgement time.
RETURN_CODE	CHAR(2)	A code indicating the status of the file being acknowledged. Values: 00 – File was successfully received and verified. 01 – Header record count does not match the number of detail records found in the file. 02 – Detail record(s) found with invalid data. 03 – Not Used. 04 – Transaction Reconciliation File (or Correction Reconciliation File) does not match corresponding Transaction File (or Correction File). 05 – Duplicate file sequence number. 06 – Gap in sequence number. 07 - Invalid ZIP file or other file structure defect Refer to Appendix C for the processing rules associated with the various RETURN_CODE values.
DELIMITER	CHAR(1)	LF
Detail Total	**77**	

11.5 Processing Requirements:

1. This file shall contain a single record only. For each file received by the From Agency/Facility Operator, the From Agency/Facility Operator shall generate an Acknowledgement File and transmit the file back to the To Agency/Facility Operator.

2. The FILE_DATE and FILE_TIME fields shall be used by the To Agency/Facility Operator as the acknowledgement date/time of the transmitted file. The To Agency/Facility Operator shall be able to support an optional ‘grace period’ (for each From Agency/Facility Operator) which the To Agency/Facility Operator shall add to the FILE_DATE and FILE_TIME to use as the acknowledgement date/time.

3. The From Agency/Facility Operator should generate a report showing any detail records that were skipped due to invalid data (RETURN_CODE = ‘02’) and should have this report available for the To Agency/Facility Operator if needed.

12.0 Transmission Methodology

1. The files shall be transmitted on a nightly basis.
2. Transmission shall be via FTP.
3. Upon completion of each file's transmission, the sending entity shall transmit a 'check' file whose name shall be comprised of the name and file type of the file to which it is associated but with a file extension of 'CHECK' (e.g., {FILE_NAME}_{FILE_TYPE}.CHECK). The receiving entity shall wait until it detects the presence of the 'check' file to begin processing the associated data file. For example, after the Tag Status File 004_19971201041015.FTAG is transmitted, the sending Agency shall transmit a 'check' file of 004_19971201041015_FTAG.CHECK. The 'check' file shall contain a single 80 character record whose contents shall be the name and extension of the file for which the 'check' file is associated.

   This will eliminate the situation where a receiving entity begins processing a file before its transmission was complete.

13.0 Modification History

Changes from FO 1.51d to FO 1.51e (06/19/2014)

1. Added Processing Requirement #6 to Section 5.5 of the FO Tag Status File clarifying the tag status values that should be included by the Host CSC into the FO Tag Status File.
2. Added Processing Requirement #3 to Section 8.5 of the FO Transaction Reconciliation File clarifying what the Facility Operator should do with transactions reconciled with ETC_POST_STATUS values of DECL or NOCC.
3. Added Processing Requirement #5 to Section 9.5 of the FO Correction File clarifying the process used by a Facility Operator to resubmit transactions reconciled with ETC_POST_STATUS values of DECL or NOCC.

Changes from FO 1.51c to FO 1.51d (07/31/2006)

4. Added Processing Requirement #2 to the FO Transaction Reconciliation File clarifying the purpose of the RJIN code.
5. Corrected File Naming convention of the FO Correction Reconciliation File to be “Home” agency and not “Host” agency. Made corresponding correction to Header Structure File Layout definition.
6. Added Processing Requirement #2 to the FO Correction Reconciliation File clarifying the purpose of the RJIN code

Changes from FO 1.51b to FO 1.51c (03/08/2002)

1. Corrected the record length for the FO Distribution File detail record (Section 7.4).
2. Corrected the record length for the FO Transaction Reconciliation File detail record (Section 8.4).
3. Added Processing Requirement #4 to the FO Correction File (Section 9.5) to indicate that the file can only contain records for transactions previously submitted via an FO Transaction File.
4. Corrected the FO Correction Reconciliation File header record (Section 10.4) field FTXN_FILE_NUM to be ITXN_FILE_NUM as described in the text (Section 10.3)
5. Corrected the record length for the FO Correction Reconciliation File detail record (Section 10.4).
6. Updated the list of RETURN_CODE values in the Acknowledgement File (Section 11.4) to coordinate with the IAG specs. Added Appendix C to described the processing rules for the various RETURN_CODE values.

Changes from FO 1.51a to FO 1.51b (12/10/2001)

1. Updated the Reporting Requirements (Section 3.0) to provide for a more comprehensive collection of settlement reports for Transactions and Corrections.
2. Modified the FO Distribution File so that it could be used for both Transaction and Correction Files.
3. Added Processing Requirement #3 to the FO Correction File to indicate that it should be split into various corrections files when transmitted to the various Home Agencies.
4. Changed the definition of the date and time fields in the FO Correction Reconciliation File to indicate the ack date of the corresponding IAG IRXN file. This ensures that settlement reports generated by the Facility Operator will tie to the IAG-3 reports for the same time period.
5. Added Processing Requirement #1 to the FO Correction File to indicate that reconciliation files should be sent to the FO as they are received from the Home Agencies.
6. Added RETURN_CODE value of ‘06’ to the Acknowledgement File in keeping with the changes in other IAG specifications.
7. Updated Appendix A to reflect the new reporting requirements.
8. Updated Appendix B to reflect the new reporting requirements.

Changes from 1.51F to FO 1.51a (08/09/2001)

1. Changed the document version naming convention from 1.51F to FO 1.51. This version becomes version FO 1.51a
2. Changed the definition of the date and time fields in the FO Transaction Reconciliation File to indicate the ack date of the corresponding IAG-INRX file. This ensures that settlement reports generated by the Facility Operator will tie to the IAG-2 reports for the same time period.
3. Modified the list of ETC_POST_STATUS code values of the FO Transaction Reconciliation File to match CSC 1.51a.
4. Added a value of '6' to the RETURN_CODE field of the Acknowledgement File to match CSC 1.51a.
5. Renamed the report generated by the Host (formally FO-1) to FH-1 (Facility Host). Adopted the naming convention of FO for those reports generated by the Facility Operator.
6. Added to the appendix, three reports required of the facility operator, FO-1 and FO-2 and FO-3. These reports are discussed in section 3.0.
7. Clarifications and typo corrections

Changes from 1.50F to 1.51F (01/07/2001)

1. No changes. Version number changed for consistency with IAG file spec.

Changes from 1.40 to 1.50F (10/23/2000)

1. Removed the transaction processing requirement from section 2.0 that required the conversion of a "credit card" account to a "cash" account if a direct credit card charge was declined. This is method of handling accounts is considered to be CSC specific and not an IAG issue.

2. Redefined the TAG_ACCT_INFO field in the FO Tag Status File as a free field for use by the Host and Facility Operator.

3. Added reconciliation codes RJIN and RJCK to the FO Transaction Reconciliation File.

4. Added the columns Trans Fee and Srvc Fee to the Facility Operator Period Summary Report shown in Appendix A. Inclusion of these columns is left to the discretion of the Host agency. Added text to describe the report.

5. Removed Appendix A (Agency Codes); Appendix B (Plaza Codes) and Appendix D (Transaction Flow) as this same information is in the IAG Inter-CSC file spec. The Facility Operator Period Summary Report is now Appendix A.

6. Corrected various typos and used *n* as opposed to N to represent a variable.

A. Host Reports

Report FH-1

Ver 1.51b

Facility Operator Period Transaction Summary Report
INRX Files Acknowledged in:
Settlement Period: 01/01/2001 to 01/31/2001

Report Date: 02/05/2001 15:32
Generated by Host Agency: New York State Thruway Authority
Non-Toll Transaction payments due to Facility Operator: Albany Airport

Agency Name	Agency Code	Total Trans	Trans Fee	PSNT Count	PSNT AMT	Srvc Fee	DECL Count	DECL AMT	NOCC Count	NOCC AMT	Reject Count	Reject AMT
Regional Consortium	022	1207		1194	35503.10		3	170.00	3	30.00	7	131.50
New York State Thruway Authority	004	4057		4049	89100.00		2	40.00	1	10.00	5	136.00
◆												
◆												
◆												
Port Authority of New York and New Jersey	005	850		846	21970.00		5	200.00	3	21.00	1	45.00
Total		6114		6089	146573.10		10	410.00	7	61.00	13	312.50

This report ties directly to IAG-2N (Reconciliation Report) with the exception of the Trans Fee (Transaction Fee) and Srvc Fee (Service Fee) columns which represent the fee charged to the Facility Operator by the Host and are not necessarily the same as those reflected in IAG-2N. The inclusion of the Trans Fee and Srvc Fee columns is optional in this report.

Report FH-2

Ver 1.51b

Facility Operator Period Correction Summary Report
IRXN Files Acknowledged in:
Settlement Period: 01/01/1999 to 01/31/1999

Report Date: 02/05/1999 15:32
Generated by Host Agency: New York State Thruway Authority
Non-Toll Correction payments due to Facility Operator: Albany Airport

Agency	Agency Code	Total Count	PSNT			Final Reject Count	Final Reject AMT
			ORG	NEW	NET		
Regional Consortium	022	5	24.00	35.00	11.00	0	0.00
New York State Thruway Authority	004	4	10.00	8.00	(2.00)	1	3.00
◆	◆	◆	◆	◆	◆	◆	◆
◆	◆	◆	◆	◆	◆	◆	◆
◆	◆	◆	◆	◆	◆	◆	◆
Port Authority of NY/NJ	005	###,###	###,###.##	###,###.##	###,###.##	###,###	###,###.##
Settlement Total		109			159.00	1	3.00

This report ties directly to IAG-3N (Correction Reconciliation Report).

B. Facility Operator Reports

Report FO-1

Ver 1.51b

Facility Operator Period Transaction Summary Report
FNRX Files with corresponding INRX Acknowledged in:
Settlement Period: 01/01/2001 to 01/31/2001

Report Date: 02/05/2001 15:32
Generated by Facility Operator : Albany Airport
Non-Toll Transaction payments due to from Host: New York State Thruway Authority

Agency Name	Agency Code	Total Trans	Trans Fee	PSNT Count	PSNT AMT	Srvc Fee	DECL Count	DECL AMT	NOCC Count	NOCC AMT	Reject Count	Reject AMT
Regional Consortium	022	1207		1194	35503.10		3	170.00	3	30.00	7	131.50
New York State Thruway Authority	004	4057		4049	89100.00		2	40.00	1	10.00	5	136.00
◆	◆	◆		◆	◆		◆	◆	◆	◆	◆	◆
◆	◆	◆		◆	◆		◆	◆	◆	◆	◆	◆
◆	◆	◆		◆	◆		◆	◆	◆	◆	◆	◆
Port Authority of New York and New Jersey	005	850		846	21970.00		5	200.00	3	21.00	1	45.00
Total		6114		6089	146573.10		10	410.00	7	61.00	13	312.50

Report FO-2

Ver 1.51b

Facility Operator Period Correction Summary Report
FRXN Files with corresponding IRXN Acknowledged in:
Settlement Period: 01/01/1999 to 01/31/1999

Report Date: 02/05/1999 15:32
Generated by Facility Operator: Albany Airport
Non-Toll Correction payments from Host Agency: New York State Thruway Authority

Agency	Agency Code	Total Count	PSNT			Final Reject Count	Final Reject AMT
			ORG	NEW	NET		
Regional Consortium	022	5	24.00	35.00	11.00	0	0.00
New York State Thruway Authority	004	4	10.00	8.00	(2.00)	1	3.00
◆	◆	◆	◆	◆	◆	◆	◆
◆	◆	◆	◆	◆	◆	◆	◆
◆	◆	◆	◆	◆	◆	◆	◆
Port Authority of NY/NJ	005	###,###	###,###.##	###,###.##	###,###.##	###,###	###,###.##
Settlement Total		109			159.00	1	3.00

Report FO-3

Ver 1.51b

Facility Operator Transaction Reconciliation Detail Report
FNRX Files with corresponding INRX files acknowledged in:
Settlement Period: 01/01/1999 to 01/31/1999

Report Date: 02/05/1999 15:32
Generated by Facility Operator: Albany Airport
Non-Toll Transaction payments from Home Agency: Regional Consortium
Due to Host Agency: NYS Thruway Authority
For payment to Facility Operator - Albany Airport

FNRX_FILE	INRX ACK Date	Total Trans Count	Trans Fee	PSNT Count	PSNT AMT	SVC Fee @ 2.30%	DECL Count	DECL AMT	NOCC Count	NOCC AMT	Other Reject Count	Other Reject AMT
022_128_19990102010901.FNRX	1/3/99	31		29	1,086.00						2	48.00
022_128_19990105012448.FNRX	1/7/99	56		55	557.20						1	45.00
022_128_19990106011057.FNRX	1/8/99	75		75	662.30							
022_128_19990106011458.FNRX	1/8/99	07		07	425.80							
022_128_19990107022140.FNRX	1/9/99	59		59	1,014.40							
022_128_19990107215531.FNRX	1/9/99	55		55	957.30							
022_128_19990109022225.FNRX	1/11/99	22		22	839.70							
022_128_19990110051614.FNRX	1/12/99	08		08	847.10							
022_128_19990110052141.FNRX	1/12/99	33		33	668.80							
022_128_19990110220253.FNRX	1/12/99	56		56	1,008.30							
022_128_19990111215735.FNRX	1/13/99	41		41	1,022.70							
022_128_19990112215445.FNRX	1/14/99	82		82	843.20							
022_128_19990114215618.FNRX	1/16/99	6		6	21.60							
022_128_19990114215902.FNRX	1/16/99	12		12	1,506.70							
022_128_19990114220222.FNRX	1/16/99	65		65	887.20							
022_128_19990115220013.FNRX	1/17/99	34		34	1,509.30							
022_128_19990116215041.FNRX	1/18/99	55		55	1,088.80							
022_128_19990118215434.FNRX	1/20/99	83		83	1,595.30							
022_128_19990120214231.FNRX	1/22/99	87		85	1,057.50				2	20.00		
022_128_19990123031220.FNRX	1/25/99	28		27	5,277.50		1	50.00				
022_128_19990123215019.FNRX	1/25/99	29		24	1,416.20		2	120.00			3	38.50
022_128_19990124215314.FNRX	1/26/99	90		90	1,692.50							
022_128_19990125215216.FNRX	1/27/99	06		04	1,273.40				1	10.00	1	0
022_128_19990128015547.FNRX	1/30/99	30		30	1,417.90							
022_128_19990129215839.FNRX	1/31/99	69		69	1,741.80							
022_128_19990129220005.FNRX	1/31/99	29		29	1,507.60							
022_128_19990130215427.FNRX	1/31/99	58		58	1,756.30							
022_128_19990131215514.FNRX	1/31/99	01		01	1,820.70							
Settlement Total		1207		1194	35,503.10		3	170.00	3	30.00	7	131.50

Report FO-4

Ver 1.51b

Facility Operator Correction Reconciliation Report
FRXN Files with corresponding IRXN files acknowledged in:
Settlement Period: 01/01/1999 to 01/31/1999

Report Date: 02/05/1999 15:32
Generated by Facility Operator: Albany Airport
Non-Toll Correction payments from Home Agency: Regional Consortium
Due to Host Agency: New York State Thruway Authority
For payment to Facility Operator: Albany Airport

	IRXN ACK Date	Total Count	PSNT			Final Reject Count	Final Reject AMT
			ORG	NEW	NET		
FRXN_FILE							
022_128_19990102010901.FRXN	01/02/1999	5	24.00	35.00	11.00	0	0.00
022_128_19990105012448.FRXN	01/05/1999	4	10.00	8.00	(2.00)	1	3.00
022_128_19990106011057.FRXN	01/06/1999	100	825.00	975.00	150.00	0	0.00
Settlement Total		109			159.00	1	3.00

C. Acknowledgement File Return Codes

	Acknowledgement File Return Codes							
	00	**01**	**02**	**03**	**04**	**05**	**06**	**07**
	Successfully Received and Verified	**Header/Detail Count Discrepancy**	**Invalid Detail Records Found**	**n/a**	**Recon File does not match the transaction file**	**Duplicate File Sequence Number**	**Gap in Sequence Number**	**Bad Zip File and Other Issue**
FNTX	Process	Do not process (2)(4)	Do not process (1)(2)(4)	n/a	n/a	Do not process (2)(4)	Process (6)	Do not process (2)(4)
FTXN	Process	Do not process (2)(4)	Do not process (1)(2)(4)	n/a	n/a	Do not process (2)(4)	Process (6)	Do not process (2)(4)
FNDX	Process	Do not process (2)(4)	Do not process (1)(2)(4)	n/a	Do not process (2)(4)	Do not process (2)(4)	n/a	Do not process (2)(4)
FNRX	Process	Do not process (2)(4)(5)	Do not process (1)(2)(4)(5)	n/a	Do not process (2)(4)(5)	Do not process (2)(4)(5)	n/a	Do not process (2)(4)(5)
FRXN	Process	Do not process (2)(4)(5)	Do not process (1)(2)(4)(5)	n/a	Do not process (2)(4)(5)	Do not process (2)(4)(5)	n/a	Do not process (2)(4)(5)
FTAG	Process	Do not process (3)(6)	Do not process (1)(3)(6)	n/a	n/a	n/a	n/a	Do not process (2)(4)

Notes:

(1) Receiving Agency/CSC needs to indicate at least the first invalid record in a report which can be made available to the Originating Agency/CSC

(2) Originating Agency should rename new file (including Header) to be unique

(3) Receiving Agency/CSC should utilize the previous valid file. Originating/Receiving Agency/CSC should escalate after x days.

(4) Originating Agency/CSC should investigate, repair file as needed and resend

(5) File should not be included on any settlement reports

(6) Originating Agency/CSC should investigate

Parking Access and Revenue Control System—Design, Installation & Maintenance

Attachment V
Non Disclosure Agreement

Good Afternoon:

As per the attached instructions, please have a principal of your company complete the attached NDA. The individual who signs the NDA on behalf of the company must sign an Exhibit A.

- All prime employees that will come in contact with information must sign an Exhibit A.
- Any sub-contractors/sub-consultant entities that will come in contact with information must sign an Exhibit B.
- The individual who signs an Exhibit B on behalf of a sub-contractor/sub-consultant must also sign an Exhibit A.
- Any employees of an entity that signs an Exhibit B that will come in contact with information must also sign an Exhibit A.
- The NDA, Exhibit A, and Exhibit B are all contained within the same attachment.
- Below are instructions that are intended to supplement the NDA instructions included. In the event of any conflict between these instruction and the attached NDA instructions, the NDA instructions prevail. For your convenience, some of the spaces have been pre-populated.

Instructions for Prime Companies:

NDA

In [1], please insert the name of your company in "all caps." In [2], insert the day of the month the agreement is being signed, in [3] please insert the month the agreement is being signed, [4] has been pre-populated with the year 2014. In [5] please insert the name of your company in "all caps." This should match [1]. In [6], please insert the company's full street address (no PO BOXES). [7] has been pre-populated with information about the project. The appropriate Port Authority contact information has been filled in for you in [8a], [8b], [8c]. Please print our name in [9], your title in [10] and the date the agreement was signed in [11]. [11] should be the same as the date filled in spaces [2], [3], and [4].

Exhibit A

After filling out and signing the NDA, the individual who signed the NDA and all other individuals who will come in contact with information must fill out and sign an Exhibit A.

All individuals who are employed by a Prime Company and will come in contact with information should follow the following steps:

In Exhibit A, please insert your name in [1], your working title (Project manager, Civil Engineer, President, etc.) in [2], and the name of your company in [3]. In [4] please insert the name of your company. [3] and [4] should be the same. In [5a], and [5b] please insert the month and date. [5c] has

been pre-populated with 2014. Please write “Port Authority” in [6]. Please print your name in [7] and insert the date Exhibit A was signed [8].

Instructions for Companies Serving as Sub-Consultant/Sub-Contractors:

Exhibit B

Please fill out an Exhibit B, as follows: In [1] please insert your name. In [2] please insert your title. In [3] please insert the full name of your entity (the company name). In [4] please insert the tupe of entity Corp, LLC, etc.) and the Jurisdiction of Formation (state). In [5] please insert the full address of the entity. In Number [6], describe the scope of work of your entity (the work being performed for the prime). [7] has been pre-populated with the information about this project. Please enter the month of the Prime Company’s NDA in [8a] and the day of the month of the Prime Company’s NDA in [8b]. [8c] has been pre-populated with 2014. In [9] please write the name of the Prime Company, print your name in [10] and insert the date the Exhibit B is being signed in [11]. After filling out and signing the Exhibit B, the individual who signed the Exhibit B and all other individuals who will come in contact with information must fill out and sign an Exhibit A.

Exhibit A

All individuals who are employed by a Sub-Contractor/Sub-Consultant and will come in contact with information should follow the following steps:

In Exhibit A, please insert your name in [1], your working title (Project manager, Civil Engineer, President, etc.) in [2], and the name of your company in [3]. In [4] please insert the name of the Prime Company. In [5a] and [5b] please insert the month and date that the Prime Company’s NDA was signed. [5c] has been pre-populated with the year 2014. Please insert the name of the Prime Company in [6]. Number [4] and [6] should be the same. Please print your name in [7] and insert the date Exhibit A was signed [8].

Thank you.

Jeanette Anderson
Procurement Contracts Manager
Procurement Department

NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT
BETWEEN

[1]_____

AND

THE PORT AUTHORITY OF NEW YORK AND NEW JERSEY

THIS NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT (this "**Agreement**") is made as of this [2]_____ day of [3]_____, [4]_____, by and between **THE PORT AUTHORITY OF NEW YORK AND NEW JERSEY** (the "**Port Authority**") a body corporate and politic created by Compact between the States of New York and New Jersey, with the consent of the Congress of the United States, and having an office and place of business at 225 Park Avenue South, New York, New York, 10003, and [5]_____ having an office and place of business at [6]_____ ("**Recipient**").

WHEREAS, the Port Authority desires, subject to the terms and conditions set forth below, to disclose to Recipient Protected Information (as defined below) in connection with [7]_____Parking Access and Revenue Control System Design, Installation and Maintenance____ (collectively, the "Project(s)", or "Proposed Project(s)"); and

WHEREAS, the Recipient acknowledges that the Port Authority, in furtherance of its performance of essential and critical governmental functions relating to the Project, has existing and significant interests and obligations in establishing, maintaining and protecting the security and safety of the Project site and surrounding areas and related public welfare matters; and

WHEREAS, in furtherance of critical governmental interests regarding public welfare, safety and security at the Project site, the Port Authority has collected information and undertaken the development of certain plans and recommendations regarding the security, safety and protection of the Project site, including the physical construction and current and future operations; and

WHEREAS, the Port Authority and Recipient (collectively, the "**Parties**") acknowledge that in order for Recipient to undertake its duties and/or obligations with regard to its involvement in the Project, the Port Authority may provide Recipient or certain of its Related Parties (as defined below) certain information in the possession of the Port Authority, which may contain or include protected, confidential, privileged, classified, commercial, proprietary or sensitive information, documents and plans, relating to the Project or its occupants or other matters, the unauthorized disclosure of which could result in significant public safety, financial and other damage to the Port Authority, the Project, its occupants, and the surrounding communities; and

WHEREAS, Recipient recognizes and acknowledges that providing unauthorized access to, or disclosing such information to third parties in violation of the terms of this Agreement

could compromise or undermine the existing or future guidelines, techniques and procedures implemented for the protection against terrorist acts or for law enforcement, investigation and prosecutorial purposes, and accordingly could result in significant irreparable harm and injury; and

WHEREAS, in order to protect and preserve the privilege attaching to and the confidentiality of the aforementioned information as well as to limit access to such information to a strict need to know basis, the Port Authority requires, as a condition of its sharing or providing access to such protected, confidential, privileged, classified, commercial, proprietary or sensitive information, documents and plans, that the Recipient enter into this Agreement and that its Related Parties thereafter acknowledge and agree that they will be required to treat as strictly confidential and/or privileged any of such information so provided, as well as the work product and conclusions of any assessments and evaluations or any recommendations relating thereto, and to also fully comply with applicable federal rules and regulations with respect thereto; and

WHEREAS, as a condition to the provision of such information to Recipient and certain Related Parties, the Recipient has agreed to enter into this Agreement with respect to the handling and use of such information and to cause Related Parties to join in and be bound by the terms and conditions of this Agreement.

NOW, THEREFORE, in consideration of the provision by Port Authority of Information for Project Purposes (as each such term is defined below) and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged by the Recipient and each Related Party that receives such Information, the Recipient and each such Related Party agrees, as follows:

1. **Defined Terms**. In addition to the terms defined in the Recitals above, the following terms shall have the meanings set forth below:

(a) **"Authorized Disclosure**" means the disclosure of Protected Information strictly in accordance with the Confidentiality Control Procedures applicable thereto: (i) as to all Protected Information, only to a Related Party that has a need to know such Protected Information strictly for Project Purposes and that has agreed in writing to be bound by the terms of this Agreement by executing a form of Acknowledgment as set forth in Exhibit A or Exhibit B, as applicable; and (ii) as to Confidential Privileged Information, only to the extent expressly approved in writing and in advance by the Port Authority, and then only the particular Confidential Privileged Information that is required to accomplish an essential element of the Project.

(b) "**Information**" means, collectively, all information, documents, data, reports, notes, studies, projections, records, manuals, graphs, electronic files, computer generated data or information, drawings, charts, tables, diagrams, photographs, and other media or renderings containing or otherwise incorporating information that may be provided or made accessible at any time, whether in writing, orally, visually, photographically, electronically or in any other form or medium, including, without limitation, any and all copies, duplicates or extracts of the foregoing.

(c) "**Protected Information**" means and includes collectively, Confidential Information, Confidential Privileged Information, Sensitive Security Information (SSI), Critical Infrastructure Information (CII) or Health Insurance Portability and Accountability Act (HIPPA) Information and Information that is labeled, marked or otherwise identified by or on behalf of the Port Authority so as to reasonably connote that such information is confidential, privileged, sensitive or proprietary in nature. The term Protected Information shall also include all work product that contains or is derived from any of the foregoing, whether in whole or in part, regardless of whether prepared by the Recipient, the Port Authority or others, or when the Port Authority receives such information from others and agrees to treat such information as Protected. The following Information shall not constitute Protected Information for the purpose of this Agreement:

(i) Particular Information, other than Confidential Privileged Information, that is provided to the Recipient by a source other than the Port Authority, provided that such source is not subject to a confidentiality agreement, or similar obligation, or understanding with or for the benefit of the Port Authority, with respect to such Information and that the identity of such source is not itself part of such Protected Information.

(ii) Information that is or becomes generally available to the public other than as a result of a disclosure by the Recipient or a Related Party in violation of this Agreement.

(iii) Information that is known to or was in the possession of the Recipient or a Related Party on a non-confidential basis prior to the disclosure of such Information by the Port Authority.

(d) "**Confidential Information**" means and includes collectively, any and all Information, documents and materials entitled to protection as a public interest privilege under New York State law and as may be deemed to be afforded or entitled to the protection of any other privilege recognized under New York and/or New Jersey state laws or Federal laws. It also includes information that contains sensitive financial, commercial or other proprietary business information concerning or relating to the Port Authority, its projects, operations or facilities that would be exempt from release under the Port Authority Freedom of Information Code.

(e) "**Confidential Privileged Information**" means and includes collectively, (i) Information that reveals security risks, threats, vulnerabilities, documentation that identifies specific physical security vulnerabilities or revealing specific security vulnerabilities details related to emergency response protocols, egress plans, flow paths, egress capacities, (diagrams, codes, standards) etc., which is not publicly available." and any and all Information, documents and materials entitled to protection as a public interest privilege under New York State law and as may be deemed to be afforded or entitled to the protection of any other privilege recognized under New York and/or New Jersey state laws or Federal laws, and (ii) certain Critical Infrastructure Information.

(f) "**Confidentiality Control Procedures**" means procedures, safeguards and requirements for the identification, processing, protection, handling, care, tracking and storage of Protected Information that are required under applicable federal or state law, the Port Authority Handbook, or by the terms of this Agreement.

(g) "**Critical Infrastructure Information**" (CII) has the meaning set forth in the Homeland Security Act of 2002, under the subtitle Critical Infrastructure Information Act of 2002 (6 U.S.C. §131-134), and any rules or regulations enacted pursuant thereto, including, without limitation, the Office of the Secretary, Department of Homeland Security Rules and Regulations, 6 C.F.R. Part 29 and any amendments thereto. CII may also be referred to as "Protected Critical Infrastructure Information" or "PCII", as provided for in the referenced rules and regulations and any amendments thereto.

(h) "**Sensitive Security Information**" (SSI) has the definition and requirements set forth in the Transportation Security Administrative Rules & Regulations, 49 CFR 1520, (49 U.S.C. §114) and in the Office of the Secretary of Transportation Rules & Regulations, 49 CFR 15, (49 U.S.C. §40119).

(i) "**Health Insurance Portability and Accountability Act**" (HIPAA) Information Employees, associates or other contract personnel who have access to Protected Health Information (PHI) must refer to, and comply with, the Privacy Policies and Procedures to Protect Personal Health Information. Privacy regulations issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA" or "Privacy Laws") place restrictions on the Group Health Plans of the Port Authority and PATH (the "Plans") ability to use and disclose Protected Health Information ("PHI").

(j) "**Port Authority Handbook**" means The Port Authority of New York and New Jersey. Information Security Handbook, as may be amended by the Port Authority, from time to time.

(k) **"Project Purposes**" means the use of Protected Information strictly and only for purposes related to Recipient's and its Related Parties' participation and involvement in the Project, and only for such period of time during which Recipient and its Related Parties are involved in Project related activities.

(l) "**Related Party**" and "**Related Parties**" means the directors, employees, officers, partners or members of the Recipient, as applicable, and the Recipient's outside consultants, attorneys, advisors, accountants, architects, engineers or subcontractors or sub-consultants (and their respective directors, employees, officers, partners or members) to whom any Protected Information is disclosed or made available.

2. **Use of Protected Information**. All Protected Information shall be used by the Recipient in accordance with the following requirements:

(a) All Protected Information shall be held in confidence and shall be processed, treated, disclosed and used by the Recipient and its Related Parties only for Project Purposes and in accordance with the Confidentiality Control Procedures established pursuant to Paragraph 2(c), below, including, without limitation, the Port Authority Handbook, receipt of which is

acknowledged by Recipient and shall be acknowledged in writing by each Related Party by signing the Acknowledgment attached hereto as Exhibit A or Exhibit B, as applicable, and applicable legal requirements. Protected Information may be disclosed, only if and to the extent that such disclosure is an Authorized Disclosure.

(b) Recipient and each Related Party acknowledges and agrees that (i) any violation by the Recipient or any of its Related Parties of the terms, conditions or restrictions of this Agreement relating to Protected Information may result in penalties and other enforcement or corrective action as set forth in such statutes and regulations, including, without limitation, the issuance of orders requiring retrieval of Sensitive Security Information and Critical Infrastructure Information to remedy unauthorized disclosure and to cease future unauthorized disclosure and (ii) pursuant to the aforementioned Federal Regulations, including, without limitation, 49 C.F.R. §§ 15.17 and 1520.17, any such violation thereof or mishandling of information therein defined may constitute grounds for a civil penalty and other enforcement or corrective action by the United States Department of Transportation and the United States Department of Homeland Security, and appropriate personnel actions for Federal employees.

(c) Recipient and each Related Party covenants to the Port Authority that it has established, promulgated and implemented Confidentiality Control Procedures for identification, handling, receipt, care, and storage of Protected Information to control and safeguard against any violation of the requirements of this Agreement and against any unauthorized access, disclosure, modification, loss or misuse of Protected Information. Recipient and each Related Party shall undertake reasonable steps consistent with such Confidentiality Control Procedures to assure that disclosure of Protected Information is compartmentalized, such that all Protected Information shall be disclosed only to those persons and entities authorized to receive such Information as an Authorized Disclosure under this Agreement and applicable Confidentiality Control Procedures. The Confidentiality Control Procedures shall, at a minimum, adhere to, and shall not be inconsistent with, the procedures and practices established in the Port Authority Handbook.

(d) The Port Authority reserves the right to audit Recipient's Confidentiality Control Procedures, and those of each Related Party, as applicable, to ensure that it is in compliance with the terms of this Agreement.

(e) The Port Authority may request in writing that the Recipient or any Related Parties apply different or more stringent controls on the handling, care, storage and disclosure of particular items of Protected Information as a precondition for its disclosure. The Port Authority may decline any request by the Recipient or any of its Related Parties to provide such item of Protected Information if the Recipient or any of the Related Parties do not agree in writing to apply such controls.

(f) Nothing in this Agreement shall require the Port Authority to tender or provide access to or possession of any Protected Information to the Recipient or its Related Parties, whether or not the requirements of this Agreement are otherwise satisfied. However, if such Protected Information is provided and accepted, the Recipient and its Related Parties shall abide by the terms, conditions and requirements of this Agreement.

(g) The Recipient and each Related Party agrees to be responsible for enforcing the provisions of this Agreement with respect to its Related Parties, in accordance with the Confidentiality Control Procedures. Except as required by law pursuant to written advice of competent legal counsel, or with the Port Authority's prior written consent, neither the Recipient, nor any of the Related Parties shall disclose to any third party, person or entity: (i) any Protected Information under circumstances where the Recipient is not fully satisfied that the person or entity to whom such disclosure is about to be made shall act in accordance with the Confidentiality Control Procedures whether or not such person or entity has agreed in writing to be bound by the terms of this Agreement or any "Acknowledgement" of its terms or (ii) the fact that Protected Information has been made available to the Recipient or such Related Parties, or the content or import of such Protected Information. The Recipient is responsible for collecting and managing the Acknowledgments signed by Related Parties pursuant to this Agreement. Recipient shall, at the Port Authority's request, provide the Port Authority a list of all Related Parties who have signed an Acknowledgment, and copies of such Acknowledgments.

(h) As to all Protected Information provided by or on behalf of the Port Authority, nothing in this Agreement shall constitute or be construed as a waiver of any public interest privilege or other protections established under applicable state or federal law.

3. **Disclosures and Discovery Requests**. If a subpoena, discovery request, Court Order, Freedom of Information Request, or any other request or demand authorized by law seeking disclosure of the Protected Information is received by the Recipient or any Related Party, Recipient shall notify the Port Authority thereof, to the extent permitted by law, with sufficient promptness so as to enable the Port Authority to investigate the circumstances, prepare any appropriate documentation and seek to quash the subpoena, to seek a protective order, or to take such other action regarding the request as it deems appropriate. In the absence of a protective order, disclosure shall be made, in consultation with the Port Authority, of only that part of the Protected Information as is legally required to be disclosed. If at any time Protected Information is disclosed in violation of this Agreement, the Recipient shall immediately give the Port Authority written notice of that fact and a detailed account of the circumstances regarding such disclosure to the Port Authority.

4. **Retention Limitations; Return of Protected Information**. Upon the earlier occurrence of either the Port Authority's written request or completion of Recipient's need for any or all Protected Information, such Protected Information, all writings and material describing, analyzing or containing any part of such Protected Information, including any and all portions of Protected Information that may be stored, depicted or contained in electronic or other media and all copies of the foregoing shall be promptly delivered to the Port Authority at Recipient's expense. In addition, as to Protected Information that may be stored in electronic or similar form, such Protected Information shall be deleted and completely removed so that such Protected Information is incapable of being recovered from all computer databases of the Recipient and all Related Parties. The Recipient may request in writing that the Port Authority consent to destruction of Protected Information, writings and materials in lieu of delivery thereof to the Port Authority. The Port Authority shall not unreasonably withhold its consent to such request. If the Port Authority consents to such destruction, the Recipient and each Related Party shall deliver to the Port Authority a written certification by Recipient and such Related Party that such Protected Information, writings and materials have been so destroyed within such period as may be

imposed by the Port Authority. Notwithstanding the foregoing, to the extent required for legal or compliance purposes, the Recipient may retain copies of Protected Information (in any format), provided that (a) the Port Authority is notified in writing of such retention, and (b) Recipient continues to abide by the requirements of this Agreement with respect to the protection of such Protected Information.

5. **Duration and Survival of Confidentiality Obligations**. The obligations under this Agreement shall be perpetual (unless otherwise provided in this Agreement) or until such time as the Protected Information is no longer considered protected, confidential and/or privileged by the Port Authority.

6. **Severability**. Each provision of this Agreement is severable and if a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

7. **Injunctive and Other Relief**. Recipient and each Related Party acknowledges that the unauthorized disclosure and handling of Protected Information is likely to have a material adverse and detrimental impact on public safety and security and could significantly endanger the Port Authority, its facilities (including, without limitation, the Project site), its patrons and the general public and that damages at law are an inadequate remedy for any breach, or threatened breach, of this Agreement by Recipient or its Related Parties. The Port Authority shall be entitled, in addition to all other rights or remedies, to seek such restraining orders and injunctions as it may deem appropriate for any breach of this Agreement, without being required to show any actual damage or to post any bond or other security.

8. **Governing Law**. This Agreement shall be governed by and construed in accordance with the laws of the State of New York, without regard to conflict of laws principles. The Port Authority (subject to the terms of the Port Authority Legislation (as defined below)) and the Recipient specifically and irrevocably consent to the exclusive jurisdiction of any federal or state court in the County of New York and State of New York with respect to all matters concerning this Agreement and its enforcement. The Port Authority (subject to the terms of the Port Authority Legislation (as defined below)) and the Recipient agree that the execution and performance of this Agreement shall have a New York situs and, accordingly, they each consent (and solely with respect to the Port Authority, subject to the terms of the Port Authority Legislation (as defined below)) to personal jurisdiction in the State of New York for all purposes and proceedings arising from this Agreement. "**Port Authority Legislation**" shall mean the concurrent legislation of the State of New York and State of New Jersey set forth at Chapter 301 of the Laws of New York of 1950, as amended by Chapter 938 of the Laws of New York of 1974 (McKinney's Unconsolidated Laws §§7101-7112) and Chapter 204 of the Laws of New Jersey of 1951 (N.J.S.A. 32:1-157 to 32:1-168).

9. **Notices**. Any notice, demand or other communication (each, a "**notice**") that is given or rendered pursuant to this Agreement by either party to the other party, shall be: (i) given or rendered, in writing, (ii) addressed to the other party at its required address(es) for notices delivered to it as set forth below, and (iii) delivered by either (x) hand delivery, or (y) nationally recognized courier service (e.g., Federal Express, Express Mail). Any such notice shall be deemed given or rendered, and effective for purposes of this Agreement, as of the date actually

delivered to the other party at such address(es) (whether or not the same is then received by other party due to a change of address of which no notice was given, or any rejection or refusal to accept delivery). Notices from either party (to the other) may be given by its counsel.

The required address(es) of each party for notices delivered to it is (are) as set forth below. Each party, however, may, from time to time, designate an additional or substitute required address(es) for notices delivered to it, provided that such designation must be made by notice given in accordance with this Paragraph 9.

Original to the Port Authority:	[8a]_____ The Port Authority of New York and New Jersey [8b]_____ [8c]_____
with a copy to:	The Port Authority of New York and New Jersey 225 Park Avenue South - 14th Floor New York, NY 10003 Attn: General Counsel's Office c/o Caroline Ioannou, Law DISO
If to the Recipient:	_____ _____ _____
with a copy to:	_____ _____ _____

10. **Entire Agreement**. This Agreement contains the complete statement of all the agreements among the parties hereto with respect to the subject matter thereof, and all prior agreements among the parties hereto respecting the subject matter hereof, whether written or oral, are merged herein and shall be of no further force or effect. This Agreement may not be changed, modified, discharged, or terminated, except by an instrument in writing signed by all of the parties hereto.

11. **Counterparts**. This Agreement may be executed in one or more counterparts, each of which shall be deemed to be an original, but all of which shall be one and the same document.

12. **Parties Bound**. This Agreement shall be binding upon the Recipient and its respective successors. The foregoing shall not be affected by the failure of any Related Party to join in this Agreement or to execute and deliver an Acknowledgement hereof.

13. **Authority**. The undersigned individual(s) executing this Agreement on behalf of the Recipient below represent(s) that they are authorized to execute this Agreement on behalf of the Recipient and to legally bind such party.

14. **Disclosure of Ownership Rights or License**. Nothing contained herein shall be construed as the granting or conferring by the Port Authority of any rights by ownership, license or otherwise in any Information.

15. **No Liability**. Neither the Commissioners of the Port Authority, nor any of them, nor any officer, agent or employee thereof, shall be charged personally by the Recipient with any liability, or held liable to the Recipient under any term or provision of this Agreement, or because of its execution or attempted execution or because of any breach, or attempted or alleged breach thereof.

16. **Construction**. This Agreement is the joint product of the parties hereto and each provision of this Agreement has been subject to the mutual consultation, negotiation, and agreement of the parties hereto, and shall not be construed for or against any party hereto. The captions of the various sections in this Agreement are for convenience only and do not, and shall not be deemed to, define, limit or construe the contents of such Sections.

RECIPIENT:

Signature: _____

Print Name: [9]_____

Title: [10]_____

Date: [11]_____

EXHIBIT A

ACKNOWLEDGMENT BY RELATED PARTY INDIVIDUAL

I, [1]_____ ("**Related Party**"), am employed as a(n) [2]_____ by [3]_____. I have been provided with and have read the Non Disclosure and Confidentiality Agreement between [4]_____ (the "**Recipient**") and The Port Authority of New York and New Jersey (the "**Port Authority**") dated [5a] _____[5b]_____, [5c]_____ (hereinafter the "**Agreement**"), and the Port Authority Handbook attached to the Agreement. I understand that because of my employer's relationship with [6]_____, both my employer and I may be provided with access to, and/or copies of, sensitive security materials, protected or confidential information. If it is required for me to review or receive Protected Information, as it is defined in the aforementioned Agreement, I acknowledge that I will be bound by each and every term and provision contained therein, and that failure to do so may include, but is not limited to, the imposition of disciplinary action and sanctions, and/or the institution of legal action seeking injunctive relief, monetary and/or criminal penalties for violation of law and/or Port Authority policies and procedures, as well as for violation of federal and/or state regulations.

To the extent that I am currently in the possession of, or have previously come into contact with, marked information as it relates to the aforementioned Agreement, I agree to conform my handling procedures for Protected Information to the practices and procedures set forth and defined herein, or risk loss of access to said Information, removal from said Project and/or subjecting myself to the aforementioned disciplinary actions and/or civil and criminal penalties.

Signature: _____

Print Name: [7]_____

Date: [8]_____

EXHIBIT B

ACKNOWLEDGMENT BY RELATED PARTY ENTITY

The undersigned, [1]_____, is the [2]_____ of [3]_____, a [4]_____ ("**Related Party**"), located at [5]_____, and is duly authorized to execute this Acknowledgment on behalf of the above Related Party. The above Related Party is involved with the functions of [6]_____ in connection with [7]_____ for The Port Authority of New York and New Jersey (the "**Port Authority**"). I acknowledge and confirm that the above named Related Party has been provided with a copy of and shall be bound and shall abide by all of the terms, requirements and conditions set forth in the Non Disclosure and Confidentiality Agreement dated [8a]_____] - [8b]_____, [8c]_____, between [9]_____ (the "**Recipient**") and the Port Authority (hereinafter the "**Agreement**"), and by the Port Authority Handbook described in the Agreement. Appropriate and responsible officers and employees of the Related Party have carefully read and understand the terms and conditions of the Agreement. The Related Party has notice and acknowledges that any breach or violation of such terms, requirements and conditions may result in the imposition of remedies or sanctions as set forth or otherwise described therein against such Related Party.

Signature: _____

Print Name: [10]_____

Date: [11]_____

Parking Access and Revenue Control System—Design, Installation & Maintenance

Attachment W
Cloud Computing Framework

THE PORT AUTHORITY OF NEW YORK & NEW JERSEY

Cloud Computing Framework

Technology Department

Updated:

2/3/2016

Version:

1.2

THE PORT AUTHORITY OF NY & NJ

The Agency's Cloud Framework consists of components and/or controls that must be addressed when selecting a Public Cloud service or Software as a Service (SaaS) vendor. The elements in this framework are dynamic and will evolve over time to ensure a secure and robust Cloud Computing environment for the Agency's business

Intentionally Left Blank

REVISON HISTORY

Version	REVISION DATE	REVISION DESCRIPTION	REVISION TRACKING NOTES
1.0	12/14/2015	Baseline Draft Version	
1.1	12/17/2015	Reformatting Document	Added Document Template
1.1.1	12/17/2015	Incorporated Department Comments	Included new Password Policy Language
1.2	02/03/2016	Incorporated Audit Document Revised Checklist (1/26/2016)	Modified Cover page

The Agency's Cloud Framework consists of components and/or controls that must be addressed when selecting a Public Cloud service or Software as a Service (SaaS) vendor. The elements in this framework are dynamic and will evolve over time to ensure a secure and robust Cloud Computing environment for the Agency's business. The Framework elements consist of the following components and/or controls:

1. Cloud Offering:

a. Government Cloud Service offering instead of Commercial Cloud.

2. The Agency Cloud Framework:

The Framework is meant to ensure that all physical, logical and information assets are secure and that security and privacy are maintained using de-facto best practices aligned with Federal Information Processing Standards (FIPS) as well as NIST Publications. To that end, Cloud Solutions should be compliant with the latest versions of the following best practices (as appropriate for application risk), to name a few:

a. NIST 800-144: Guidelines on Security and Privacy in Public Cloud Computing
b. FIPS 199: Standards for Security Categorization of Federal Information and Information System
c. FIPS 200: Minimum Security Requirements for Federal Information and Information Systems
d. NIST 800-53: Recommended Security Controls for Federal Information Systems and Organizations
e. NIST 800-146: Cloud Computing Synopsis and Recommendations
f. Cloud Security Alliance: Cloud Controls Matrix Version 3.0 (CCMv3)

3. For Software-as-a-Service (SaaS), excerpt from NIST 800-146:

a. **Data Protection**. Analyze the SaaS provider's data protection mechanisms, data location configuration and database organization/transaction processing technologies, and assess whether they will meet the confidentiality, compliance, integrity and availability needs of the Agency.

b. **Client Device/Application Protection**. Consistent with the FIPS 199 impact level of the data being processed, protect the Agency's client device (e.g., a computer running a Web browser) so as to control the exposure to attacks.

c. **Encryption**. Require that strong encryption using a robust algorithm with keys of required strength be used for Web sessions whenever the subscribed SaaS application requires the confidentiality of application interaction and data transfers. Also require that the same diligence be applied to stored data. Federal agencies must employ government-approved cryptographic algorithms for encryption and digital signature, and the implementations need to be FIPS 140-2 validated. Understand how cryptographic keys are managed and who has access to them. Ensure that cryptographic keys are adequately protected.

d. **Secure Data Deletion**. Require that cloud/vendor providers offer a mechanism for reliably deleting data at the Agency's request.

4. Data Location:

a. Must be US-based, in multiple locations for redundancy and administered by US Citizens.

5. Electronic Discovery:

a. A cloud/vendors information archival capabilities must preserve the original metadata of 'client data' so as to not adversely affect the Agency's litigation risk

6. Data Ownership:

The Agency retains exclusive ownership over all its data:

a. That the cloud/vendor provider acquires no rights or licenses to that data, including intellectual property rights or licenses.
b. The cloud/vendor may not use the Agency's data for its own purposes;
c. and that the cloud/vendor does not acquire and may not claim any interest in the data due to security.

7. Availability:

a. Must meet 99.9% uptime

8. Physical Security:

a. 24-hour monitoring of data centers.
b. Multi-factor authentication, including biometric scanning for data center access.

c. Internal data center network is segregated from the external network.
d. Role separation renders location of specific customer data unintelligible to the personnel that have physical access.
e. Faulty drives and hardware are demagnetized and destroyed.

9. Logical Security:

a. Lock box processes for strictly supervised escalation process greatly limits human access to your data.
b. Servers run only processes on whitelist, minimizing risk from malicious code.
c. Dedicated threat management teams proactively anticipate, prevent, and mitigate malicious access.
d. Port scanning, perimeter vulnerability scanning, and intrusion detection prevent or detect any malicious access.

10. Data Security:

a. Encryption at rest protects the Agency's data on cloud/vendor servers.
b. Encryption in transit with SSL/TLS protects Agency's data transmitted between the Agency and cloud/vendor application.
c. Threat management, security monitoring, and file/data integrity prevents or detects any tampering of data.

11. Compliance Standards:

a. **Health Insurance Portability and Accountability Act (HIPAA):** HIPAA imposes, under law, certain requirements for security, privacy, and reporting regarding the processing of electronic protected health information.

b. **Federal Information Security Management Act (FISMA):** requires U.S. federal agencies to develop, document, and implement controls to secure their information and information systems. Federal Risk and Authorization Program (FedRAMP) is a federal risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services.

c. **ISO 27001 Certification:** Along with NIST 800-53, ISO 27001 is one of the best security benchmarks available. Cloud/vendor should comply with the set of physical, logical, process and management controls defined by ISO 27001:2013, inclusive of ISO 27018 Privacy controls.

d. **European Union (EU) Model Clauses:** The EU Data Protection Directive, a key instrument of EU privacy and human rights law. The EU model clauses are recognized as a preferred method for legitimizing the transfer ofpersonal data outside the EU for cloud computing environments. Supporting the EU model clauses involves investing and building the operational controls and processes required to meet the exacting requirements of the EU model clauses. Unless a cloud/vendor service provider is willing to agree to the EU model clauses,the Agency might lack confidence that it can comply with the EU Data Protection Directive's requirements for the transfer of personal data from the EU to jurisdictions that do not provide "adequate protection" for personal data.

e. **U.S.–EU Safe Harbor framework:** The U.S.-EU Safe Harbor framework also enables the Agency, as needed, to legally transfer personal data outside of the EU under the EU Data Protection Directive.

f. **Statement on Standards for Attestation Engagements No. 16 (SSAE 16):** Cloud/vendor has been audited by independent third parties and can provide SSAE16 SOC 1 Type I and Type II and SOC 2 Type II reports on how the service implements controls.

g. **Canadian Personal Information Protection and Electronic Documents Act (PIPEDA):** The Canadian Personal Information Protection and Electronic Documents Act pertains to how private sector organizations collect, use, and disclose personal information in the course of commercial business.

h. **Gramm–Leach–Bliley Act (GLBA):** The Gramm–Leach–Bliley Act requires financial institutions to put processes in place to protect their clients' nonpublic personal information. GLBA enforces policies to protect information from foreseeable threats in security and data integrity.

12. Audit Control Requirements[1]:

a. General:

1. Documented procedures, flowcharts and process maps for the application.
2. Conduct regular audits, vulnerability testing, and security scanners.
3. SSAE 16 SOC 2 Type II (previously known as SAS 70 Level 2)
4. Federal Risk and Authorization Management Program (FedRAMP) Certification
5. ISO27001 Certification
6. Criminal Justice Information Services (CJIS) security policies and procedures compliant for law enforcement information and systems.
7. Background check should be performed on all personnel.

b. System/Security Administration

1. Administrative personnel should receive training.
2. Administrative staff should receive general security awareness training before access is provided. All security training must be reinforced at least every three years and must be tracked as per the PA Information Security Handbook.
3. System and security administration procedures should be documented and distributed.
4. Administrator(s) roles and responsibilities should be documented.
5. Developers and/or programmers should not have access to the production server.
6. Operating system administrators should not have access to the production database and application.

c. Hardening of operating system/database that supports the application:

1. Disable and/or remove unnecessary ports/services.
2. Remove all manufacturer samples from the production system. Scripts must be removed from production systems, except those required for the operation and maintenance of the system.
3. Default, public, and guest accounts should be secured/locked/removed.
4. Change all default passwords; delete all default content and login scripts.
5. Limit administrative and user account privilege and access.
6. Document system accounts like administrator, root, oracle, and sys.
7. Document user/group access rights
    a. Users/groups should be setup with least access required to perform job responsibilities.
8. Implement access control at the database level (i.e. user roles and permissions, passwords, secure links)
9. Use secure encrypted remote access methods.
10. If the application is a web application, log (and monitor) web traffic and trend the activity looking for abnormal activity.
11. Ensure that appropriate security and vulnerability assessment tools are running.
12. At login, last user login should not display.
13. Inventory listing of hardware and software should be current and maintained.

d. License Management:

1. Ensure that application licensing requirements are documented, reviewed and maintained.
2. Application licenses should be current/valid and individuals/groups with application access should have completed the necessary access request forms and adhere to licensing requirements.

e. Logical Access Controls:

1. All users are required to read the Agency Policy Computing Resource Administrative Instruction (AI 15-4.03) and sign an acknowledgement of the Agency IT Acceptable Use Code of Conduct policy prior to account activation.
2. Procedures to grant/modify/delete access should be documented.
    a. Access request forms for adding/modifying/deleting users should be used.
    b. Account expiration for contractors and consultants.
    c. Accounts adequately identify the user – no generic accounts

[1] Audit Department 1/26/2016 Update, with TEC Department modifications to password policies

3. Ensure that security administrator procedures exist to:
    a. Create/remove application access in a timely manner
    b. Review user roles/permissions
4. Validate that all users have accessed the application within the past 90 days.
    a. Review dormant accounts
    b. Inactive accounts should be removed.
5. Each user has a unique user ID as described in the Port Authority Standard and Guidelines.
    a. All user accounts profile should include Employee ID# and full user name.
6. Roles are setup with least access required to perform job responsibilities.
7. Roles should have a segregation of duties/roles.
8. All accounts must have an individual or business group assigned to be responsible for account management.
9. Segregation of duties and areas of responsibility must be implemented where appropriate.
10. Whenever segregation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, audit trails and management supervision. The PA must approve these compensating controls.
11. Review of audit trails and system approvals must be performed independent and retained to document the implementation of these security controls
12. Access Control List (ACL) should include:
    a. Current list of ACL
    b. Creation and updates to ACL
    c. Testing and approvals of ACL
13. The application should have the PA's warning banner on the login screen. The application has a warning banner, terms of use, and/or privacy statement that was approved by the Port Authority on the login screen.
14. The system should have an access role that would allow real only access to all application, database and operating system screens, functions, logs and reports.
15. Remote access should be approved, secured, and documented in accordance with PA policy. Remote access, at a minimum, must consist of multifactor authentication mechanisms, secured communications (TLS/ VPN encryption methodology), access control mechanisms and logging of user activity.

f. Password Controls: (see Section 14. Port Authority Password Policies and Requirements)

g. Application Controls:

1. Data Validation & Input Controls
    a. The application should have input controls to verify the validity of the data entered.

2. Data Retention and Management
    a. All data should be classified according to its sensitivity (confidential, etc) and protected accordingly.
    b. Data archive strategy should be documented and in place.
        i. Should specify how long active data is kept.

4. Data Integrity and Security
    a. Sensitive data, such as credit card #s and social security #s, should be encrypted.
    b. Data should be restricted and audit trails should be available to identify all user activity include view access to sensitive data.
    c. Data should be stored in the database encrypted and blocked from user views in the application unless it is authorized.
    d. Encryptions level at a minimum should be AES 256bit when encryption is used.

5. Application Interfaces:
    a. Interface file should be secured and archived.
    b. Reconciliation of data should be done on a batch record and totals. Detail data reconciliations should be completed on periodic basis.

6.Processing Controls:

a. Application databases/interfaces should have the necessary controls to prevent processing of inaccurate, duplicate, or unauthorized transactions and producing inaccurate outputs.
b. Controls to ensure that all data is processed and accounted for should be in place.
c. Rejected items should be logged, tracked and resolved in a timely manner.

h. Change Management:

1. Processes and tools should be used to report, track, approve, fix, and monitor changes on the application.
2. The application and all changes to the application should be tested before being put into production.
   a. Documentation of approval for change and evidence of testing should be in place.
   b. Specific timetable/schedule should be documented.
3. Emergency procedures should be documented and distributed.
4. Separate environments are required for development, test, quality assurance, production.
5. Procedures should require that no changes be made directly in the production environment without going through the development/test/quality assurance environments.
6. Formal change control procedures for all systems must be developed, implemented and enforced.
7. Where technically feasible, development software and tools must not be maintained on production systems.
8. Source code for application or software must not be stored on the production system running that application or software.
9. Privileged access to production systems by development staff must be restricted.

i. Application Logging, Audit Trails and Record Retention:

1. Audit trails for operating, application, and database systems should exist and reviewed.
2. Users and roles should be tracked and reviewed
   a. Maintain documentation
3. All failed logon attempts should be logged.
4. All sensitive transactions and changes should be logged and an audit trail created.
5. Audit trails should contain who made the change, when it was made, and what was changed.
6. Only the security administrator should have access to change or delete these logs or audit trails.
7. Audit trails should be reviewed by the business owner(s) and security administrator.
8. Management reporting should be produced through the application.
9. Access reports by user and privilege should be produced and reviewed periodically including access violation reports and exception transaction reporting.

j. Contingency Planning, Disaster Recovery and Backup Management:

1. A business contingency plan and a disaster recovery plan for the application should be documented and stored off-site, including escalation plan and current call tree.
2. Plans should be tested and the outcomes of the tests (success/failure) should be documented.
3. Regular backups of the application and the application data should be stored off-site.
4. Application executables should be stored off-site or in escrow.
5. Application configurations should be documented and backed-up.
6. Full system backup should be encrypted.
7. Backup procedures should be documented.
8. Tape maintenance should include:
   a. Periodically testing integrity of tape
   b. Procedures for tape destruction due to faulty or scratched hardware.

k. Performance Monitoring:

1. Incident monitoring procedures should be documented and incidents logs should be reviewed to ensure that appropriate action is taken.
2. Performance statistics should be examined and reviewed periodically by system administrators/business owner(s).

3. If vendor(s) support the application, a service level agreement for uptime, performance monitoring, updates, etc should be confirmed.
4. Baseline tools or security products should be used and checked on a quarterly basis.

l. Patch Management:

1. Patch management procedures and documentation
   a. Procedures should include testing, approvals, and distribution.
   b. Documentation should include emergency procedures.
2. Apply all new patches and fixes to operating system and application software for security.
3. All security patches must be reviewed, evaluated and appropriately applied in a timely manner. This process must be automated, where technically possible.

m. Physical Protection:

1. Physical access to the application hardware should be appropriately restricted.
   a. Physical access secured by single authentication mechanism i.e. swipe card.
   b. Physical security adequate for equipment (locked cabinets)
2. Appropriate fire suppression systems should be in place.
3. Environmental condition adequately controlled (no water, dirt, clutter) and monitored.
   a. Temperature and humidity monitoring should be implemented.
4. Security cameras installed in sensitive areas
5. Power surge protection and emergency power backup are in place.
6. All hardware and software assets must be inventoried.
7. Visitors including maintenance personnel, to data center, server and network equipment storage facilities must be escorted at all times.

n. Anti-virus Management / Integrity / Vulnerability Software Management:

1. Virus patch management procedures must be documented, including emergency update procedures.
2. Anti-virus and software integrity checkers must be implemented to prevent and detect the introduction of malicious code or other threats.
3. Virus software engines and definitions must be implemented and up-to-date.
4. A remote distribution server should be implemented for virus software updates and documentation on remote distribution should be current and maintained.
5. Intrusion detection system must be in place,
6. All systems must have vulnerability scans performed before going into production and periodically thereafter. Appropriate action, such as patching or updating the system, must be taken to address discovered vulnerabilities.
7. Host-based intrusion detection/ firewalls software must be installed and enabled on all systems to protect from threats and to restrict access. Incident response procedures must be in place to address any alerts identified and system owner should be notified of alerts and what action was taken to mitigate the issues.
8. Monitoring systems must be deployed (e.g., intrusion detection/prevention systems) at strategic network locations to monitor inbound, outbound and internal network traffic.
9. Monitoring systems must be configured to alert incident response personnel to indications of compromise or potential compromise.
10. Procedures must be established to maintain information security during an adverse event.
11. Firewalls should be implemented.
12. Firewall rules documentation should be up-to-date.
13. Network management connections must be performed from a secure, dedicated network.
14. Network authentication is required for all devices connecting internal networks.

o. Wireless Device:

1. Devices should be using WPA/WPA2 and AES encryption or better.
2. Devices should disallow broadcasting of the SSID.
3. All default parameters should be changed.
4. Devices should have MAC address filtering enable or some type of authentication mechanism in place.

p. Web Application Vulnerabilities and Controls:

1. Best Practice and Standards:
   a. The Open Web Application Security Project (OWASP) - www.owasp.org
   b. www.webappsec.org (a consortium of web application security professionals)
   c. Center for Internet Security (CIS) – www.cisecurity.org
2. Perform data validation & integrity checks for field values and ensure the HTML special characters are stripper for all HTML request.
3. Do not allow site pages to be cached by user browsers.
4. All sensitive, personal or confidential data (including SSN, passwords, session IDs for sensitive applications, confidential or sensitive business transactions, etc.) should be transmitted between browser and server within an SSL-encrypted session (or other encrypted transmission) and are encrypted in the database at rest.
5. All sensitive and personal data should be masked and encrypted were possible.
6. Legal Issues:
   a. The site should have a privacy statement and term of usage.
   b. American Disability Act – Section 508 should be considered during the development process due to the requirement that federal agencies' electronic and information technology is accessible to people with disabilities.
7. Web Authentication: To prevent passwords from being passed in the clear, have authentication occur within an TLS encrypted tunnel. Use TLS (certificate) to protect the password.
8. Password Reset:
   a. For internal applications, reset passwords via the helpdesk or security administrator of the site
   b. For external applications, send temporary password to known e-mail address, that must be changed upon login and/or
   c. Have customer service reset after the user has been validated.
   d. If possible, use two factor authentication like Secure ID fobs.

q. Credit Card Processing Checklist:

1. If credit cards are accepted, PCI Standards (PCI DSS v3.1) should be followed and the process should be PCI compliant. Ensure all vendors and consultants are required to be PCI compliant. Attachment - The payment card application should be PCI compliant (PA-DSS v3.1).
2. A segregated network and/or an approved Point of Sale terminal should be in place for the system or terminal used to process credit card transactions.
3. The credit card processor standard and requirements should be followed, i.e. maintain transaction data for two years.
4. Maintain the security of the customer information, including not storing credit numbers, the cardholder CVC/CVV numbers or any of the data from the magnetic strip on the credit card.
5. Maintain the transaction data for contesting chargebacks, ensure that the processor fees are appropriate and do reconciliations of the transactions processed and the money deposited in the Port Authority bank accounts.
6. The appropriate Port Authority functional areas should be made aware credit card processing activity and should be involved applying for the Merchant ID for MasterCard/Visa, Discover and American Express.
7. Create a privacy policy and procedure for staff and consultants.
8. Perform quarterly vulnerability scans of the network that contains the credit card processing, annual PCI reviews according to the PCI DSS, and annual system penetration testing.
9. Perform the appropriate annual assessment and provide a report on compliance (ROC) which state shows compliance.

r. Credit Card Processing Checklist:

1. The Disaster Recovery plan should include at a minimum the following areas.
   a. Business Impact Analysis
   b. Critical Time Frame
   c. Application System Impact Statements

d. Recovery Strategy & Approach
e. Recovery Time Objectives (RTO)/Recovery Point Objectives (RPO) for all critical systems.
f. Disaster Definition
g. Detailed Recovery Steps for each Disaster Definition
h. Escalation Plans and Decision Points
i. System Components- An inventory of the criticality of systems (including but not limited to software and operating systems, firewalls, switches, routers and other communication equipment).
j. Disaster Recovery Emergency Procedures
k. Plan Procedure Checklist
l. Disaster Recovery Team Organization
    i. Salvage Team & Team Responsibilities
    ii. Disaster Recovery Responsibilities
    iii. Essential Position – Require back-up personnel to be assigned.
m. Contacts information Disaster Recovery Team and critical vendors - this area should be reviewed semi-annually for updates and changes.
n. Post-Disaster – Detail what steps need to be taken to move from disaster mode back to normal operations.

2. Contingency plans (e.g., business continuity plans, disaster recovery plans, and continuity of operations plans) must be established and tested regularly.
3. Backup copies of procedures, software, and system images should be taken regularly and moved offsite.
4. Backups and restoration must be tested regularly.

13. Criminal Justice Information Services (CJIS) Compliance (as appropriate).

14. Port Authority (PA) Password Policies and Requirements:

These requirements applies to all PA information technology systems regardless of whether they are administered by (or on behalf of) the PA.

1. End user accounts will be disabled (not deleted) after 60 days of non-use;
2. All information technology system account passwords will be complex:
    a. a minimum of 10 characters in length
    b. contain at least two upper and lowercase alphabetic characters,
    c. contain at least one number (0-9)
    d. contain at least one special character (e.g.- + } : > _ ? & $ % #)[2]
    e. Smartphones, where capable, shall leverage biometric access to provide the most security for the least inconvenience.
3. User passwords will require a change every 90 days.
4. All accounts will be granted the minimum level of access and permissions necessary to perform an assignment.
5. If a system account fails to satisfy the requirements of this policy, an administrator may place the account in “disabled” status until remedied.
6. Changes to an account’s access privileges require the appropriate managers to request new or modified access.
7. All users are required to read the Agency Computing Resource Administrative Instruction and sign an acknowledgement of the Agency IT Acceptable Use Code of Conduct policy prior to account activation.
8. Annually, all managers are required to certify that only authorized employees have accounts on Agency systems. Technology and the Office of the CSO will work with managers to provide them with the lists of employees and their accounts.

[2] Example: W0nD3rFu!l

9. Passwords must not be shared.
10. Accounts should be locked after a three logon failures.
11. Passwords should not be the same account name.
12. No concurrent login capabilities.
13. Password file should be securely stored with limited access and encrypted.
14. Application forces initial passwords to be changed and the initial passwords should not be easily guessable.
15. Set "automatic session timeout" to 15 minutes of inactivity and require user to log back in with valid ID and password.

Purpose of the following items:

(1) so we don't create 'islands' of users without a centralize mechanism to manage accounts and
(2) protecting our *information* assets, regardless of where it may reside (in cloud, on premises, etc..)

15. Integration with the Agency's Active Directory platform for centralized account/application user management
16. Integration with the Agency's Information Rights Management Framework which will leverage Microsoft Azure Rights Management Services

Parking Access and Revenue Control System—Design, Installation & Maintenance

Attachment X
Qualification Requirements

ATTACHMENT X – QUALIFICATION REQUIREMENTS

General Note – All customer references must be employees of that company.

a) The Proposer shall have had at least three (3) years of continuous experience immediately prior to the date of the submission of its proposal in the management and operation of at least one Parking Access and Revenue Control System (PARCS), which includes design, implementation and maintenance. The Proposer may fulfill this prerequisite if it can demonstrate that the persons or entities owning and controlling the Proposer have had a cumulative total of at least the same number of years and type of direct continuous experience immediately prior to the submission of this proposal as is required of the Proposer, or has owned and controlled other entities which meet the requirement.

#	Customer Company Name	Description of Services Provided		Start Date (MM/YYYY)	End Date (MM/YYYY)
1					
		Contact Name	Contact Email	Contact Phone	
	Primary Contact				
	Alternate Contact				

Description of Scope		
Contract at least three (3) years of continuous experience immediately prior to the date of the submission of its proposal? **(Y/N)**		
System installed in the Continental United States? **(Y/N)**		
Estimated Contract value		
Contract includes design **(Y/N)**		
Contract includes implementation **(Y/N)**		
Contract includes maintenance **(Y/N)**		
Contract includes testing **(Y/N)**		
Contract includes training **(Y/N)**		

b.) During the time period stated in (a) above, the Proposer shall demonstrate satisfactory performance of at least two (2) contracts for similar services of similar scope supporting airport parking facilities that process at least 2,500,000 parking and revenue transactions annually and/or have at least 7,000 parking spaces.

Based on these requirements, fill out the table below.

Requirement	Contract 1	Contract 2
Customer Company Name		
Contract Start Date		
Contract End Date		
Description of Scope		
Contract within the last 3 years? **(Y/N)**		
System installed in the Continental United States? **(Y/N)**		
Estimated Contract value		
Contract includes purchase of equipment **(Y/N)**		
Contract includes installation **(Y/N)**		
Contract includes testing **(Y/N)**		
Contract includes training **(Y/N)**		
Contract includes maintaining equipment **(Y/N)**		

Requirement	Contract 1	Contract 2
Contract includes system integration? **(Y/N)**		
Contract includes implementation? **(Y/N)**		

ATTACH DOCUMENTATION CERTIFYING AND SUPPORTING THESE PREREQUISITES